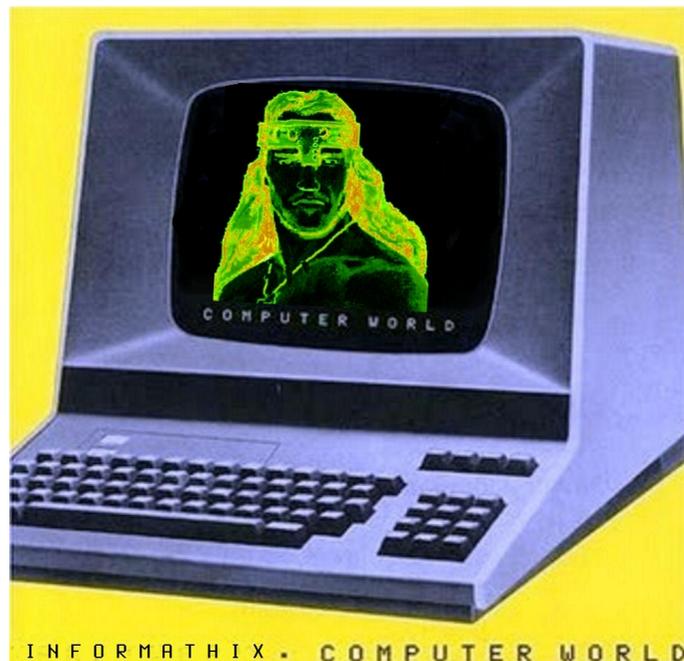


Mathématiques

IUT INFO1 / 2011-2012

Licence Creative
Commons   

IUT
d'informatique
de Nantes
1^{ère} année



Guillaume CONNAN et Thierry BRUGÈRE



UNIVERSITÉ DE NANTES

TABLE DES MATIÈRES

1	Langages, grammaires, automates, logique	132
1.1	Approche historique	133
1.2	Les machines de TURING	133
1.2.1	Description sommaire	133
1.2.2	Un exemple pour découvrir	133
1.2.3	Définitions	135
1.2.4	Fonctions MT-calculables	135
1.2.5	Fonctions récursives	137
1.3	Langages	139
1.3.1	Un exemple pour découvrir	139
1.3.2	Définitions et notations	141
1.3.3	Langages	143
1.3.4	Langages et expressions rationnels (ou réguliers)	144
1.4	Automates	147
1.4.1	Définitions	147
1.4.2	Langage reconnaissable	148
1.4.3	Langage reconnu par un automate fini	149
1.4.4	Automates équivalents	150
1.4.5	Automates standards	151
1.4.6	Automates émondés	151
1.4.7	Automates déterministes	153
1.4.8	Opérations rationnelles sur les automates	154
1.4.9	Théorème de KLEENE	155
1.4.10	Automate associé à un langage défini par une expression rationnelle	155
1.4.11	Automates à états finis avec sortie	156
1.4.12	Automates à pile	156
1.4.13	Machines de TURING : le retour	158
1.5	Présentation générale de la logique des propositions	159
1.5.1	Syntaxe	159
1.5.2	Sémantique	160
1.6	EXERCICES	161
1.6.1	Machines de TURING	161
1.6.2	Fonctions récursives	161
1.6.3	Langages	164
1.6.4	Langages et expressions rationnels	165
1.6.5	Généralités sur les automates	166
1.6.6	Expression rationnelle associée à un automate	166
1.6.7	Automates standards et émondés	167
1.6.8	Automates déterministes	167
1.6.9	Construction d'automates	168
1.6.10	Automates à états finis avec sortie	168
1.6.11	Automates à pile	168

1 Langages, grammaires, automates, logique



Nous essaierons dans ce chapitre de découvrir comment parler à une machine?...

L'ensemble des symboles $\{0, 1, \varepsilon\}$ forme un **alphabet**.

Le pointeur indique la première case. Nous voudrions par exemple changer les 0 en 1 et vice-versa puis remettre le pointeur dans sa position initiale.

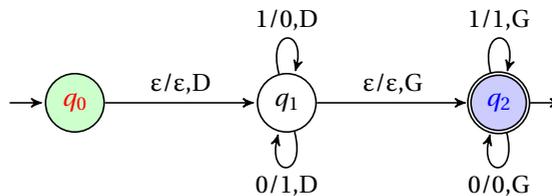
Il est possible d'effectuer trois actions qui dépendent de l'état du pointeur et du caractère pointé :

- changer l'état du pointeur ;
- changer le caractère pointé sur le ruban ;
- déplacer le pointeur d'une case vers la gauche ou vers la droite.

L'algorithme est donc :

- lorsque le pointeur rencontre le premier blanc, il se déplace vers la droite ;
- chaque fois que le pointeur rencontre un 0 ou un 1, il le change en son complémentaire et se déplace vers la droite ;
- lorsqu'il rencontre le deuxième blanc, il recule d'une case vers la gauche jusqu'à ce qu'il rencontre le premier blanc.

Ceci constitue un algorithme que nous prendrons l'habitude de représenter par l'**automate** suivant :



Les cercles correspondent aux différents états de la machine : il y en a trois. Les flèches décrivent, elles, les actions accomplies par la machine.

La flèche entrante en q_0 indique qu'il s'agit de l'état initial. Le double cercle autour de q_2 indique qu'il s'agit de l'état final.

Une flèche allant de q_i à q_j surmontée d'un couple $a/b, c$ signifie que si la machine est dans l'état q_i et qu'elle pointe sur une case contenant a alors elle remplace a par b et bouge d'une case vers la direction indiquée par c : Gauche, Droite, Reste sur place.

On voit qu'un nombre fini d'instructions permet de traiter une chaîne de longueur aussi longue que l'on veut.

2 3 Définitions

Machine de TURING

Une machine de TURING standard (il en existe d'autres) est un triplet :

$$M = (Q, X, \varphi)$$

où

- Q est un ensemble fini appelé *alphabet d'état* ;
- X est un autre ensemble fini appelé *alphabet de ruban* ;
- φ est une fonction de domaine $D \subseteq Q \times X$ et à valeurs dans $Q \times X \times \{G, R, D\}$ avec G, R, D les options du mouvement du pointeur (gauche, reste immobile, droite).

On choisira en général Q et X de telle sorte que leur intersection soit vide. Quelques éléments particuliers :

- $q_0 \in Q$ est l'*état initial* ;
- $Q_f \subseteq Q$ est l'*ensemble des états finaux* ;
- $\varepsilon \in X$ est le symbole blanc.

Définition 1 - 1

Cela donne, avec les données de l'exemple précédent, $Q = \{q_0, q_1, q_2\}$, $X = \{\varepsilon, 0, 1\}$, $Q_f = \{q_2\}$ et la fonction φ est définie à l'aide du tableau suivant :

$\varphi(q_i, x)$	q_0	q_1	q_2
ε	(q_1, ε, D)	(q_2, ε, G)	
0		$(q_1, 1, D)$	$(q_2, 0, G)$
1		$(q_1, 0, D)$	$(q_2, 1, G)$

En fait, une machine de TURING agit sur des *mots* construits à partir d'un *alphabet*. Un alphabet est en fait un ensemble fini. Définissons un peu mieux ce que peut être un mot :

Soit X un alphabet. Soit λ le mot ne comportant aucun caractère. L'ensemble X^* des mots construits avec l'alphabet X est défini par :

1. $\lambda \in X^*$;
2. si $a \in X$ et $m \in X^*$, alors le mot construit à partir de m en ajoutant a à droite est un mot de X^* ;
3. μ est un élément de X^* seulement s'il peut être obtenu à partir de λ par application de l'étape 2 un nombre fini de fois.

Définition 1 - 2

On peut donc à l'aide de cette définition construire un mot en ajoutant un par un des éléments de l'alphabet. Nous devons donc créer une fonction plus rapide pour créer des mots :

Concaténation

Soient m_1 et m_2 deux mots de X^* . La **concaténation** de ces deux mots est le mot $m_1 m_2 \in X^*$ obtenu en écrivant m_2 à la suite de m_1 .

Définition 1 - 3

2 4 Fonctions MT-calculables

La notion de fonction calculable par une fonction de TURING est primordiale en informatique. Une telle fonction sera dite **MT-calculable**.

Cette notion peut paraître assez abstraite alors mieux vaut étudier un exemple avant de l'affronter.

Par exemple, nous allons construire une machine de TURING qui calcule le successeur de la représentation unaire d'un entier.

Définition 1 - 4

Représentation unaire d'un entier

Un nombre entier $n \in \mathbb{N}$ a pour représentation unaire 1^{n+1} c'est-à-dire la concaténation de $n + 1$ symboles de l'alphabet $X = \{1\}$.

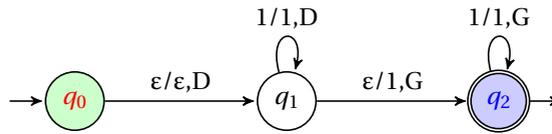
Ainsi, la représentation de 0 est 1, celle de 1 est 11, celle de 2 est 111, etc.

On notera \bar{n} la représentation de l'entier n .

Ainsi, le successeur de n est obtenu en ajoutant un 1 à son écriture unaire.

Décrivons une machine de TURING qui calcule cette fonction :

- la fonction successeur s est définie sur $D = \{\lambda, \varepsilon 1 \varepsilon, \varepsilon 11 \varepsilon, \varepsilon 111 \varepsilon, \dots\}$: l'entrée sur le ruban est donc la représentation unaire du nombre n précédée du symbole ε , toutes les autres cases étant occupées par des ε ;
- l'alphabet de ruban est $X = \{1, \varepsilon\}$;
- l'alphabet d'état est $\{q_0, q_1, q_2\}$;
- $Q_f = \{q_2\}$;
- la fonction φ est décrite par l'automate suivant :



La configuration initiale est le mot $q_0 \varepsilon \bar{n} \varepsilon$.

Le pointeur rencontre le premier blanc et change donc d'état et se dirige vers la droite jusqu'à rencontrer un deuxième blanc qui est alors remplacé par un 1. Le pointeur change d'état et se déplace vers la gauche tant qu'il pointe sur un 1.

La machine s'arrête lorsqu'elle rencontre à nouveau un blanc car $\varphi(q_2, \varepsilon)$ n'est pas définie.

La configuration finale est $q_2 \varepsilon \bar{n} 1 \varepsilon$.

Cela vous aidera alors peut-être à comprendre la définition d'une fonction MT-calculable :

Fonction MT-calculable

Soit $f : D \subseteq X^* \rightarrow X^*$ une fonction et $M = (Q, X, \varphi)$: une machine de TURING. M calcule f si :

- il existe une unique transition de q_0 et que sa forme est $\varphi(q_0, \varepsilon) = (q_i, \varepsilon, D)$ avec $q_i \neq q_0$ (il faut quitter l'état initial à partir de ε) ;
- il n'existe pas de transition de la forme $\varphi(q_i, x) = (q_0, x', m)$ avec $i \neq 0$, $(x, x') \in X^2$ et $m \in \{G, R, D\}$ (il ne faut pas revenir à l'état initial) ;
- il n'existe pas de transition de la forme $\varphi(q_f, \varepsilon)$ où $q_f \in Q_f$ (il ne faut pas que la machine continue à fonctionner dans son état final en présence d'un blanc car il y en a une infinité et la machine ne s'arrêterait jamais) ;
- pour tout $\mu \in D$, notons $v = f(\mu)$. Le calcul effectué par la machine M en partant de la configuration initiale $q_0 \varepsilon \mu \varepsilon$ s'arrête après un nombre fini d'étapes dans la configuration finale $q_f \varepsilon v \varepsilon$ (la machine doit calculer $f(\mu)$) ;
- le calcul ne s'arrête jamais si $\mu \notin D$ (la machine ne calcule $f(\mu)$ que si ce nombre est défini).

Définition 1 - 5

Nous définirons en TD :

- la fonction identiquement nulle ;
- la fonction addition ;
- les fonctions projections :

$$\pi_i^{(n)}(x_1, x_2, \dots, x_n) = x_i, \quad 1 \leq i \leq n$$

2 5 Fonctions récursives

Nous avons découvert des fonctions MT-calculables. Pour arriver jusqu'à la thèse de CHURCH-TURING, il faudrait déterminer quelles sont les fonctions qui sont MT-calculables. Nous allons montrer qu'il s'agit des fonctions récursives dont l'étude est donc indispensable pour étudier l'algorithmique...

2 5 1 Fonctions primitives récursives

Les fonctions de base des fonctions primitives récursives sont les fonctions précédemment étudiées :

- la fonction successeur $s : s(x) = x + 1$;
- la fonction identiquement nulle $z : z(x) = 0$;
- les fonctions projection $\pi_i^{(n)}$.

Nous appellerons **fonction arithmétique** une fonction de \mathbb{N}^k dans \mathbb{N} .

Les fonctions de base sont MT-calculables. Nous admettrons que les fonctions arithmétiques obtenues par composition et récurrence le sont aussi, en définissant ces opérations ainsi :

Composition de fonctions arithmétiques

Soient g_1, g_2, \dots, g_k k fonctions arithmétiques de k variables et h une fonction arithmétique de k variables. Soit f la fonction définie par :

$$f(x_1, x_2, \dots, x_n) = h(g_1(x_1, \dots, x_n), \dots, g_k(x_1, \dots, x_n))$$

alors f est appelée la **composition** de h et de g_1, g_2, \dots, g_n et se note :

$$f = h \circ (g_1, g_2, \dots, g_n)$$

Définition 1 - 6

Par exemple, si $h(x_1, x_2) = s(x_1) + s(x_2)$, $g_1(x) = 2x$ et $g_2(x) = x^2 + 37$ alors :

$$f(x) =$$

Récurrence

Soient g et h des fonctions arithmétiques totales de n et $n+2$ variables respectivement. La fonction f de $n+1$ variables définie par :

- $f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n)$;
- $f(x_1, \dots, x_n, y+1) = h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y))$,

est appelée **récurrence de base g et de pas h** .

On conviendra qu'une fonction de zéro variable est constante.

Définition 1 - 7

On peut alors définir les fonctions récursives primitives :

Fonctions récursives primitives

Une fonction est **primitive récursive** si elle peut être obtenue à partir des fonctions *successeur*, *zéro* et *projection* par l'application d'un nombre fini de compositions et de récurrences.

Définition 1 - 8

Par exemple, il est possible de définir l'addition de deux entiers à partir de la fonction s , des projections $\pi_1^{(1)}$ et $\pi_3^{(3)}$ et d'une récurrence de base $g(x) = \pi_1^{(1)}(x)$ et de pas $h = s \circ \pi_3^{(3)}$:

$$\begin{cases} \text{add}(m, 0) = g(m) = m \\ \text{add}(m, n + 1) = h(m, n, \text{add}(m, n)) = s(\text{add}(m, n)) \end{cases}$$

Nous verrons en exercice quelques exemples de fonctions primitives récursives.

Cependant, certaines fonctions ne le sont pas comme par exemple la fonction d'ACKERMANN :

$$\begin{cases} A(0, y) = y + 1 \\ A(x + 1, 0) = A(x, 1) \\ A(x + 1, y + 1) = A(x, A(x + 1, y)) \end{cases}$$

qui est cependant MT-calculable mais la preuve est hors de notre portée.

2 5 2 La thèse de Church-Turing

Si nous avons un peu plus de temps, nous pourrions définir les fonctions récursives (comme par exemple les fonctions primitives récursives et la fonction d'ACKERMANN) et montrer que toutes les fonctions récursives sont MT-calculables.

Ainsi les travaux de TURING tendant à définir un critère de « calculabilité » par une machine (ou un être humain muni d'une feuille et d'un crayon) rejoignent ceux de CHURCH et KLEENE sur le λ -calcul ou, ce qui revient au même, les fonctions récursives (notion introduite par GÖDEL au même moment).

C'est un domaine d'étude fort paradoxal : techniquement réduit (les machines de TURING sont simples à décrire !), il entraîne depuis 80 ans des recherches fort ardues.

Il faut cependant garder en tête que les machines de TURING sont des « humains qui calculent » comme le formulera le philosophe WITTGENSTEIN et évidemment TURING lui-même : « un être humain muni d'un papier, d'un crayon, d'un ruban et soumis à une stricte discipline est en fait une machine universelle ».

Comme tous nos ordinateurs *actuels* sont équivalents à des machines de TURING, ils sont donc également des modèles d'êtres humains en train d'effectuer des calculs de manière disciplinée mais non intelligente.

Cette notion est fondamentale également du côté matériel et du côté logiciel. Un ordinateur est une machine de TURING car, pourvu qu'on lui donne un bon code, il effectuera ce que vous voulez.

Le programmeur est lui-même une machine de TURING s'il a écrit son programme (et prouvé qu'il fonctionne...).

Un langage est une machine de TURING.

L'architecture même de l'ordinateur fonctionne selon ce principe : données et instructions sont de même nature dans la mémoire de l'ordinateur comme nombres et fonctions dans la machine de TURING.

Cependant, les machines de TURING sont des modèles théoriques (ruban infini) et donc éloignés du quotidien du programmeur. Savoir qu'il existe un algorithme qui résout notre problème est une chose, connaître sa complexité en est une autre...L'étude de la complexité des algorithmes est un domaine de recherche en soi.

Mais TURING aura surtout lancé le débat sur l'intelligence artificielle : est-ce qu'une machine sera un jour capable de raisonner comme un cerveau humain ? Il avait proposé un test : entamer un dialogue à distance avec une « entité » qui peut être un être humain ou une machine. Lorsque le comportement de la machine sera indiscernable de celui de l'être humain par ce test, alors on pourra considérer la machine aussi intelligente que l'être humain.

Cette évolution passera peut-être par une remise en cause de l'ordinateur électronique : des essais d'ordinateur à ADN sont en cours depuis une quinzaine d'années par exemple mais leur base théorique est toujours la machine de TURING...

Pour finir, une nouvelle citation de Donald E. KNUTH :

Science is what we understand well enough to explain to a computer. Art is everything else we do.

Mais trêve de philosophie, retournons à l'école maternelle et révisons notre alphabet...

3 Langages

3.1 Un exemple pour découvrir

Reconnaître des mots est une tâche très importante en informatique qu'on retrouve dans des domaines aussi divers que :

- les compilateurs qui transforment un code de haut niveau, compréhensible par un humain, en un code machine directement utilisable par l'ordinateur ;
- les éditeurs de texte et les traitements de texte ;
- les bases de données, les moteurs de recherche ;
- etc.

Nous avons déjà découvert que les machines de TURING utilisaient un *alphabet* assez sommaire pour former des *mots* ; nous avons donné des définitions générales de ces notions. Voyons à présent un exemple plus complexe correspondant plutôt à l'action d'un compilateur (votre maîtresse d'école vous a peut-être présenté les choses ainsi). Nous voudrions que l'ordinateur puisse produire la phrase suivante (ou vérifier qu'elle est « correcte ») :

LA JEUNE FILLE ÉTUDIE LE BEAU COURS.

L'*alphabet des symboles* est :

$$A = \{LA, JEUNE, FILLE, ÉTUDIE, LE, BEAU, COURS, .\}$$

Vous avez noté que le mot « alphabet » n'est pas à prendre au sens usuel du terme. Par exemple, **def**, **return**, **if**, **for** sont des éléments de l'alphabet de symboles de Python. Maintenant, ces symboles ne peuvent pas être assemblés n'importe comment ; il faut suivre les règles d'une *grammaire* dont voici un exemple :

1. <phrase> → < sujet > < verbe > < complément > < ponctuation >
2. < sujet > → < groupe nominal >
3. < complément > → < groupe nominal >
4. < groupe nominal > → < article féminin > < adjectif féminin > < nom féminin >
5. < groupe nominal > → < article féminin > < nom féminin > < adjectif féminin >
6. < groupe nominal > → < article féminin > < nom féminin >
7. < groupe nominal > → < article masculin > < adjectif masculin > < nom masculin >
8. < groupe nominal > → < article masculin > < nom masculin > < adjectif masculin >
9. < groupe nominal > → < article masculin > < nom masculin >
10. < article masculin > → LE
11. < article féminin > → LA
12. < adjectif féminin > → JEUNE

13. <adjectif masculin> → JEUNE
14. <adjectif masculin> → BEAU
15. <nom féminin> → FILLE
16. <nom masculin> → COURS
17. <verbe> → ÉTUDIE
18. <ponctuation> → .

Ici, <phrase> est l'*axiome* : c'est notre point de départ.

Les *variables* sont les termes entre <>.

Les règles 1 à 9 sont les *règles syntaxiques*, la première étant toujours l'axiome.

Les règles 10 à 18 sont les *règles lexicales*.

Le *langage engendré* par la grammaire est l'ensemble de toutes les phrases que l'on peut former en respectant les règles. Voici quelques exemples de phrases « grammaticalement correctes » comme disait votre maîtresse :

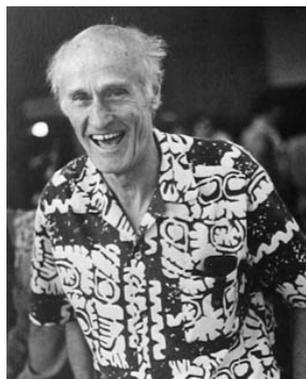
LE JEUNE COURS ÉTUDIE LA FILLE.
LA FILLE ÉTUDIE LE JEUNE COURS.
LA FILLE ÉTUDIE LE COURS.

La grammaire ne suffit pas : certaines phrases heurtent notre sens commun mais ceci est une autre histoire...

Remarque 1

Pour éviter le caractère ambigu des termes « mot », « lettre » employés dans de nombreux ouvrages et même un peu plus tôt dans ce cours, nous préférons dans le cours qui suit utiliser les termes « symbole » et « chaînes » car nous venons de voir qu'une « lettre » au sens mathématique peut être un « mot » au sens courant... De plus, les termes « caractères » et « chaînes » désignent habituellement, dans les langages informatiques, des types de variables qui correspondent aux notions que nous allons introduire.

Le domaine que nous allons étudier a été défriché par des linguistes, des mathématiciens, des informaticiens, des philosophes. Voici par exemple des portraits du linguiste Noam CHOMSKI, du mathématicien Stephen KLEENE et de l'informaticienne Sheila GREIBACH qui ont donné leur nom à de nombreuses notions que nous croiserons dans notre cours :



Noam CHOMSKI, né en 1928 et professeur de linguistique au MIT, est également connu pour son engagement politique (une recherche sur le nombre d'occurrences de la chaîne « Chomski » dans n'importe quel numéro du *Monde diplomatique* est un exercice de mise en pratique de notre cours et renverra toujours un résultat non nul...)

Stephen KLEENE (1909 - 1994) est un mathématicien américain dont nous avons déjà parlé car il a fondé la théorie de la récursion avec Alonzo CHURCH, Kurt GÖDEL et Alan TURING. Il est l'inventeur du concept d'expression rationnelle et de langage rationnel que nous retrouverons tout au long de ce cours.

Sheila GREIBACH, née en 1939 et professeur à UCLA a effectué d'importantes recherches dans le domaine des langages formels, des automates et des compilateurs.

3 2 Définitions et notations

Définition 1 - 9

Un *alphabet* est un ensemble fini non vide. Les éléments sont appelés des *symboles* ou des *caractères*.

Nous avons rencontré l'alphabet $\{\epsilon, 1, 0\}$ du ruban des machines de TURING, mais aussi l'ensemble $\{LA, JEUNE, FILLE, ÉTUDIE, LE, BEAU, COURS, \cdot\}$ dans l'exemple d'introduction. On peut aussi penser à $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, \times, -, /, (,)\}$ pour écrire des expressions arithmétiques dans \mathbb{N} , etc.

Une *chaîne* est une juxtaposition de symboles. On appelle cette juxtaposition la *concaténation*.

Plus rigoureusement :

Soit A un alphabet. Soit λ_A la *chaîne vide* (ne comportant aucun symbole).

L'ensemble A^* des chaînes construites avec l'alphabet A est défini par :

1. $\lambda_A \in A^*$;
2. si $a \in A$ et $c \in A^*$, alors la chaîne construite à partir de c en concaténant a à droite est une chaîne de A^* ;
3. μ est un élément de A^* seulement s'il peut être obtenu à partir de λ_A par application de l'étape 2 un nombre fini de fois.

Définition 1 - 10

La *longueur* d'une chaîne est le nombre de symboles qui la composent. On note souvent $|\mu|$ la longueur de la chaîne μ . En particulier $|\lambda_A| = 0$.

On note $|\mu|_a$ le nombre d'occurrences du symbole a dans la chaîne μ . On note A^n l'ensemble de toutes les chaînes de longueur n .

Par convention, $A^0 = \{\lambda_A\}$ qui n'est donc pas vide.

$A^* = \bigcup_{n \geq 0} A^n$: c'est l'ensemble de toutes les chaînes, éventuellement vides.

$A^+ = \bigcup_{n > 0} A^n$: c'est l'ensemble de toutes les chaînes non vides.

La concaténation des chaînes μ et ν sera notée $\mu\nu$.

Par exemple, si $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, +, \times, -, /, (,)\}$, alors $3 * (4 - 2) + 8$ et $)32 + - 7$ sont des chaînes de longueurs respectives 9 et 6.

Vous aurez noté que les notations rappellent la notion de fermeture transitive et transitive réflexive...

Vous aurez noté que $A^1 = A$.

Vous aurez noté que A a beau être fini, A^* est infini.

Notations

Par convention, nous noterons en général les symboles avec les premières lettres de l'alphabet latin (a, b, c, d, \dots), les chaînes avec des lettres grecques (μ, ν, ξ, \dots) et les alphabets avec des majuscules.

Remarque 2

La concaténation est une *loi de composition interne* sur A^* car en concaténant deux éléments de A^* , on obtient encore un élément de A^* .

Cette loi est également associative et possède un *élément neutre* λ . Cela confère à A^* la structure de *monoïde libre*, selon les standards informatiques. Les mathématiciens parlent de *magma associatif unitaire*. En anglais, on utilise le terme *lattice*.

L'associativité nous permet d'utiliser la notation *puissance* :

$$a^n = \underbrace{aa \dots a}_{n \text{ fois}}; a^n b^k = \underbrace{aa \dots a}_{n \text{ fois}} \underbrace{bb \dots b}_{k \text{ fois}}; (ab)^n = \underbrace{ababab \dots ab}_{n \text{ fois } ab}$$

Par convention on pose $a^0 = \lambda$ pour tout a élément de A .

Définition 1 - 11

- On dit que $\mu \in A^*$ est un *préfixe* de $v \in A^*$ si, et seulement si, il existe $\xi \in A^*$ telle que $v = \mu\xi$. Si $\xi \neq \lambda$, on dit que μ est un *préfixe propre* de v .
- On dit que $\mu \in A^*$ est un *suffixe* de $v \in A^*$ si, et seulement si, il existe $\xi \in A^*$ telle que $v = \xi\mu$. Si $\xi \neq \lambda$, on dit que μ est un *suffixe propre* de v .
- On dit que $\mu \in A^*$ est un *facteur* de $v \in A^*$ si, et seulement si, il existe $\xi \in A^*$ et $\xi' \in A^*$ telles que $v = \xi\mu\xi'$. Si $(\xi, \xi') \neq (\lambda, \lambda)$, on dit que μ est un *facteur propre* de v .
- Pour toutes chaînes μ et v de A^* , le quotient à gauche de v par μ est noté $\mu^{-1}v$ et défini par :

$$\mu^{-1}v = \begin{cases} \xi & \text{si } v = \mu\xi \\ \text{n'a pas de sens} & \text{si } \mu \text{ n'est pas un préfixe de } v \end{cases}$$

On définit de même le quotient à droite.

Si $\mu = aababc$, le quotient à gauche de μ par aab est abc .

Définition 1 - 12

Une chaîne μ étant une suite (finie) de symboles, on appelle *sous-chaîne* de μ toute sous-suite de la suite μ . Tout facteur de μ est une sous-chaîne de μ mais la réciproque est fautive, un sous mot de μ contient des lettres de μ dans le bon ordre mais pas forcément de façon consécutive.

Si $\mu = aabbaabc$, $abba$ est une sous-chaîne qui est aussi un facteur, bbb est une sous-chaîne qui n'est pas un facteur.

Définition 1 - 13

Si $\mu = a_{i_1}a_{i_2} \dots a_{i_n}$ est une chaîne de A^* , sa *transposée* (ou son image miroir) est la chaîne

$${}^t\mu = a_{i_n}a_{i_{n-1}} \dots a_{i_1}$$

Un mot qui est égal à son transposé est appelé *palindrome*.

On notera la propriété :

$${}^t(\mu\nu) = {}^t\nu{}^t\mu$$

3 3 Langages

Définition 1 - 14

Un *langage* sur A est un sous-ensemble de A^* .

Par exemple, sur l'alphabet $A = \{LA, JEUNE, FILLE, \acute{E}TUDIE, LE, BEAU, COURS, .\}$, les ensembles suivants sont des langages :

- $\{LA LA LE, LE FILLE BEAU, \acute{E}TUDIE COURS FILLE LA\}$;
- l'ensemble de toutes les cha\enes contenant « FILLE » ;
- l'ensemble de toutes les cha\enes de longueur multiple de 37.

Si nous travaillons sur l'alphabet $B = \{0, 1\}$, alors l'ensemble B^8 des cha\enes de longueur 8 est l'ensemble bien connu des octets.

Un langage \eetant d\efini comme un ensemble, il est alors naturel de s'int\eresser aux op\erations ensemblistes sur les langages. L'union, l'intersection, la compl\ementation et la diff\erence s'introduisent naturellement :

Th\eor\eme 1 - 1

Si L et L' sont deux langages sur l'alphabet A (rappel, L et L' sont deux parties de A^*) alors $L \cup L'$, $L \cap L'$, $L - L'$ et $\complement_A L = \bar{L}$ sont des langages sur A .

Notations

La r\eeunion ou l'union $L \cup L'$ est aussi not\ee $L + L'$ et on l'appelle le plus souvent la somme des langages L et L' .

Nous allons maintenant introduire deux autres op\erations fondamentales qui vont nous permettre de d\ecrire des langages int\eressants. Ces op\erations sont le **produit** ou la **concat\enation** de deux langages et l'**\eetoile** ou la **fermeture it\erative** (appel\ee aussi **\eetoile de Kleene**) d'un langage. Commen\cons par le **produit** :

D\efinition 1 - 15

Si L et L' sont deux langages sur A , on d\efinit le produit du langage L par le langage L' (attention \ l'ordre) le langage not\ee LL' ou LL' d\efini par

$$LL' = \{\mu.\mu' \mid \mu \in L \text{ et } \mu' \in L'\}$$

LL' est le langage obtenu en faisant le produit (concat\enation) de toutes les cha\enes de L avec toutes les cha\enes de L' .

LL' est bien un langage et cette op\eration est manifestement associative (l'int\er\et est de pouvoir se passer de parenth\eses). Alors :

On d\efinit r\eeursivement le langage L^n :

D\efinition 1 - 16

$$\begin{cases} L^0 = \{\lambda\} \text{ par convention (m\eme si } L = \emptyset) \\ L^{n+1} = L^n L \end{cases}$$

Pratiquement L^n n'est autre que l'ensemble des cha\enes de longueur n construites avec l'« alphabet » L . (on accepte cette vision m\eme si L est infini).

Par exemple, soient $L_1 = \{ab, ba\}$, $L_2 = \{c, cc\}$ et $L_3 = \{ac\}$. Nous avons

$$L_1 L_2 = \{abc, abcc, bac, bacc\}$$

$$L_1 L_2 L_3 = \{abcac, abccac, bacac, baccac\}$$

$$L_1^2 = \{abab, abba, baab, baba\}$$

Si $n \in \mathbb{N}^*$, $L^{<n}$ désigne le langage

Définition 1 - 17

$$L^{<n} = \bigcup_{i=0}^{n-1} L^i = L^0 \cup L^1 \cup \dots \cup L^{n-1}$$

Pratiquement $L^{<n}$ est l'ensemble des mots de longueur $< n$ que l'on peut construire avec l'alphabet L .

Par exemple, si $L = \{a, ab\}$ alors $L^{<3} = \{\lambda, a, ab, aa, aab, abab, aba\}$.

On appelle **étoile de KLEENE** ou **itération** du langage L le langage

Définition 1 - 18

$$L^* = \bigcup_{k=0}^{+\infty} L^k = \bigcup_{k \in \mathbb{N}} L^k$$

L'union de toutes les puissances strictement positives de L étant notée L^+ :

$$L^+ = \bigcup_{k \in \mathbb{N}^*} L^k \text{ et } L^* = L^+ \cup \{\lambda\}$$

Remarque 3

1. L^* désigne l'ensemble de tous les produits possibles (penser concaténation) d'éléments de L y compris la chaîne vide, pratiquement L^* est le langage défini sur l'alphabet L y compris la chaîne vide.
2. Si $L = \{\mu\}$ où μ est une chaîne de A^* on a $L^* = \{\mu^n \mid n \in \mathbb{N}\}$. Le plus souvent L^* est noté simplement μ^* , en conséquence le langage noté a^*b^* est le langage $L^*L'^*$ avec $L = \{a\}$ et $L' = \{b\}$. Nous utiliserons ces abus de notations par la suite lors de la présentation des expressions rationnelles.
3. Si $L = \{\lambda\}$ alors $L^* = \{\lambda\}$. Si $L = \emptyset$ alors $L^* = \{\lambda\}$ puisque nous avons décidé (par convention) que, pour tout langage L , nous avons $L^0 = \{\lambda\}$.
4. $L^+ = LL^* = L^*L$
5. $L^* = L^+ \cup \{\lambda\} = L^+ + \{\lambda\}$, n'oublions pas que l'union ou la réunion de deux langages est aussi notée « + ».
6. Nous conviendrons qu'en l'absence de parenthèses, l'étoile a priorité sur la concaténation qui a elle-même priorité sur la réunion.

3 4 Langages et expressions rationnels (ou réguliers)

Comme souvent en mathématiques, il n'existe pas UNE SEULE définition d'une notion mais plusieurs définitions équivalentes. C'est à l'auteur du cours de choisir UNE PARMi les différentes définitions possibles : les autres deviendront des propriétés.

3 4 1 Langage rationnel**Définition 1 - 19****Langage rationnel (ou régulier)**

Soit L un langage sur l'alphabet A . Il est dit rationnel s'il peut être obtenu récursivement uniquement à l'aide des opérations :

- réunion (somme),
- concaténation (produit),
- étoile de KLEENE

en partant :

- du langage vide \emptyset ,
- des langages du type $\{a\}$ avec $a \in A \cup \{\lambda_A\}$.

Voici un exemple pour illustrer cette notion.

Considérons l'alphabet $A = \{b, o, x\}$ et L l'ensemble des chaînes finissant par x .

Par exemple, box , $bobox$, $xxbobboxoxbbxxoxxxx$, x appartiennent à ce langage.

On peut le décrire ainsi :

$$L = (\{b\} \cup \{o\} \cup \{x\})^* \cdot \{x\}$$

C'est donc un langage rationnel car obtenu à partir de singletons et d'opérations rationnelles.

Par abus de notation, on se contentera souvent de l'écrire ainsi :

$$L = (b + o + x)^* x \quad \text{ou} \quad (b^* o^* x^*)^* x \quad \text{ou} \quad \{b, o, x\}^* x$$

Il est ensuite assez évident de montrer les propriétés suivantes :

Propriétés 1 - 1

- Tout langage **fini** est rationnel.
- Si L est rationnel, alors L^* est rationnel.
- Si L_1 et L_2 sont rationnels, alors $L_1 + L_2$ et $L_1 L_2$ sont rationnels.

3 4 2 Expression rationnelle

Ouvrons un shell bash et lançons la commande suivante :

```
$ egrep rationnel* ./logic.tex
```

On obtient :

```
l'inventeur du concept d'expression rationnelle et de langage rationnel
sentation des expressions rationnelles.
\subsection{Langages et expressions rationnels (ou réguliers)}
\subsubsection{Langage rationnel}
\begin{definition}[Langage rationnel (ou régulier)]
Soit  $L$  un langage sur l'alphabet  $A$ . Il est dit rationnel s'il peut être
C'est donc un langage rationnel car obtenu à partir de singletons et
d'opérations rationnelles.
\item Tout langage \textbf{fini} est rationnel.
\item Si  $L$  est rationnel, alors  $L^*$  est rationnel.
\item Si  $L_1$  et  $L_2$  sont rationnels, alors  $L_1 + L_2$  et  $L_1 L_2$  sont rationnels
```

On obtient alors toutes les lignes où apparaît une chaîne de préfixe « rationnel » dans le début du fichier source \LaTeX de ce document, celle-ci étant mise en gras.

La commande **egrep** permet en effet d'effectuer une recherche d'*expression rationnelle* dans un fichier. Définissons cette notion :

Expression rationnelle

Soit A un alphabet. Une expression rationnelle définie sur A est :

- \emptyset ,
- λ_A ,
- un élément quelconque de A ,
- des « formules *bien formées* » à partir des éléments de A en utilisant les opérateurs rationnels. Ainsi, si R_1 et R_2 sont des expressions rationnelles, alors $(R_1 + R_2)$, $R_1 \cdot R_2$ et R_1^* le sont aussi.

Définition 1 - 20

Disons qu'intuitivement, il s'agit de formules obéissant aux règles de « syntaxe » usuelles. Par exemple, les formules suivantes ne sont pas *bien formées* :

$$a+ \quad)a+ \star b(\quad + \star a$$

Définissons à présent l'ensemble des chaînes associées à une expression rationnelle de manière récursive :

Langage décrit par une expression régulière

À chaque expression rationnelle E on fait correspondre le langage $\mathcal{L}(E)$ de A^* défini par :

- $\mathcal{L}(\emptyset) = \emptyset$
- $\mathcal{L}(\lambda_A) = \{\lambda_A\}$
- $a \in A, \mathcal{L}(a) = \{a\}$
- $\mathcal{L}(E + E') = \mathcal{L}(E) \cup \mathcal{L}(E') = \mathcal{L}(E) + \mathcal{L}(E')$
- $\mathcal{L}(E \cdot E') = \mathcal{L}(E) \cdot \mathcal{L}(E') = \mathcal{L}(E) \mathcal{L}(E')$
- $\mathcal{L}(E^*) = \mathcal{L}(E)^*$

Propriété 1 - 2

Considérons $E = (a + b)^* \cdot c = (a + b)^* c$, et déterminons le langage $\mathcal{L}(E)$:

$$\begin{aligned} \mathcal{L}((a + b)^* \cdot c) &= \mathcal{L}((a + b)^*) \mathcal{L}(c) \\ \mathcal{L}((a + b)^* \cdot c) &= \mathcal{L}(a + b)^* \mathcal{L}(c) \\ \mathcal{L}((a + b)^* \cdot c) &= (\mathcal{L}(a) + \mathcal{L}(b))^* \mathcal{L}(c) \\ \mathcal{L}((a + b)^* \cdot c) &= (\{a\} \cup \{b\})^* \{c\} \\ \mathcal{L}((a + b)^* \cdot c) &= \{a, b\}^* \{c\} \\ \mathcal{L}((a + b)^* \cdot c) &= \{c, ac, bc, aac, aabbaabaac, bbabababc, \dots\} \end{aligned}$$

Le langage $\mathcal{L}(E)$ est l'ensemble des chaînes de la forme μc où μ est une chaîne quelconque du langage $\{a, b\}^*$ ou, si l'on préfère, μ est la chaîne vide ou une chaîne de longueur quelconque formé à l'aide des symboles a et b dans n'importe quel ordre.

Examinons de plus près l'expression rationnelle $E = (a + b)^* \cdot c$ pour appréhender rapidement le langage $\mathcal{L}(E)$ qu'elle décrit. Cette expression nous donne en fait une règle de construction des chaînes du langage $\mathcal{L}(E)$:

- on la lit de la gauche vers la droite ;
- le signe $+$ correspond au **ou** exclusif. On l'appelle parfois l'*alternative* ;
- le signe \cdot de la concaténation correspond au **et** logique ;
- le symbole \star correspond à une boucle que l'on peut ne pas faire ou faire un nombre quelconque de fois.

Les chaînes de $\mathcal{L}(E)$ vont toutes se terminer par c , les symboles qui vont précéder c sont décrits par $(a + b)^*$. Soit on ne rentre pas dans la boucle et le résultat est λ , soit on rentre dans la boucle autant de fois que l'on veut et, à chaque boucle, on choisit a ou bien b .

Inversement, on peut trouver une expression rationnelle qui correspond à un langage. Par exemple, nous pouvons décrire le langage sur $A = \{a, b, c, d\}$ constitué des chaînes qui commencent par c et qui contiennent au moins un a mais pas de d :

$$E = c(a^*b^*c^*)^* a(a^*b^*c^*)^*$$

ou bien

$$E = c(a + b + c)^* a(a + b + c)^*$$

Dans ce qui suit R, S et T sont des expressions rationnelles et l'égalité d'expressions rationnelles signifie qu'elles dénotent le même langage.

Propriétés 1 - 3

- $R + S = S + R, R + R = R$
- $R + \emptyset = R$
- $(R + S) + T = R + (S + T)$
- $R(ST) = (RS)T$
- $R\lambda = \lambda R = R$
- $R\emptyset = \emptyset R = \emptyset$
- $R(S + T) = RS + RT, (S + T)R = SR + TR.$
- $R^* = R^*R^* = (R^*)^* = (\lambda + R)^*$
- $(R + S)^* = (R^*S^*)^* = (R^* + S^*)^* = (R^*S)^* R^*$
- $R^+ = RR^* = R^*R$

Le théorème suivant relie langage et expressions rationnelles :

Théorème 1 - 2

Un langage de A^* est rationnel si, et seulement si, il est dénoté par une expression rationnelle.

En effet, la famille des langages dénotés par une expression rationnelle contient $\emptyset, \{\lambda\}$ et tous les singletons $\{a\}$ avec $a \in A$ puisqu'il a bien été précisé que tout langage fini était rationnel.

Cette famille est fermée pour l'union, le produit et l'étoile, elle contient donc l'ensemble de tous les langages rationnels définis sur A .

Réciproquement tout langage dénoté par une expression rationnelle est obtenue à partir des symboles et de la chaîne vide par une suite finie d'unions, de produits ou d'étoiles, il est donc rationnel.

4 Automates

4.1 Définitions

Nous avons déjà abordé la notion d'automates lors de l'étude des machines de TURING (cf section 1.2.2 page 134).

Nous allons généraliser cette notion grâce à la définition suivante :

Automate fini

Un automate \mathcal{A} est caractérisé par un quintuplet $\langle A, Q, I, T, \varphi \rangle$:

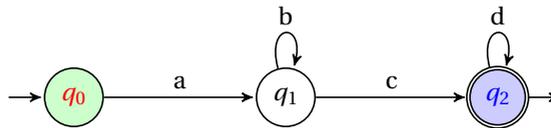
- un alphabet A appelé l'*alphabet d'entrée* ;
- un alphabet Q appelé l'*alphabet d'état* (Q est donc **fini**) ;
- une partie I non vide de Q appelée *ensemble des états initiaux* ;
- une partie T non vide de Q appelée *ensemble des états terminaux* ;
- une relation τ de $Q \times A$ vers Q ou de $Q \times (A \cup \{\lambda\})$ vers Q , appelée *relation de transition*.

Définition 1 - 21

Par exemple $\tau(q_1, a) = q_2$ signifie que quand l'automate est dans l'état q_1 et qu'il rencontre le symbole a , alors il passe dans l'état q_2 .

On a l'habitude de représenter à l'aide d'un graphe comme nous l'avons déjà vu lors de l'étude des machines de TURING.

Cette fois, les arcs vont porter les symboles de l'alphabet A (ce symbole sera nommé *étiquette de la transition*).



Ici, par exemple, on dit que (q_0, a, q_1) est une *transition* de l'automate, que a est l'*étiquette* de cette transition dont l'*origine* est q_0 et l'*extrémité terminale* est q_1 .

On pourra aussi noter cette transition $q_0 \xrightarrow{a} q_1$.

On peut aussi représenter l'automate par sa *table de transition* :

μ	q_0	q_1	q_2
a	q_1		
b		q_1	
c		q_2	
d			q_2

4 2 Langage reconnaissable

Reprenons l'automate précédent défini sur l'alphabet $A = \{a, b, c, d\}$.

Les chaînes ac , $abbbbcb$, $abbbbcbddddd$ semblent calculables par l'automate mais pas les chaînes ad , $ddddaa$, $aaabc$. L'automate étant simple, c'est assez facile à « voir ». Dans des cas plus compliqués, les mathématiques prendront le relais de nos yeux. Fabriquons donc nos « lunettes ».

Un **calcul** \mathbf{c} de l'automate \mathcal{A} (ou une exécution ou une trace de l'automate \mathcal{A}) est une suite de transitions (des relations de $Q \times A$ dans Q) telles que l'origine de chacune (sauf la première) coïncide avec l'extrémité terminale de la précédente :

$$\mathbf{c} = q_{i_0} \xrightarrow{\alpha_1} q_{i_1} \xrightarrow{\alpha_2} q_{i_2} \xrightarrow{\alpha_3} \dots \xrightarrow{\alpha_n} q_{i_n}$$

que l'on note aussi

$$\mathbf{c} = q_{i_0} \xrightarrow{\alpha_1 \alpha_2 \dots \alpha_n} q_{i_n}$$

la longueur de ce calcul étant n (il y a n transitions) et $\alpha_1\alpha_2\cdots\alpha_n$ est l'étiquette du calcul c , c 'est une chaîne de A^* . Il faut remarquer qu'un calcul a une seule étiquette mais qu'une même chaîne peut être l'étiquette de plusieurs calculs distincts.

Un calcul de \mathcal{A} est **réussi** si son origine est un état initial et son extrémité terminale un état final.

Une chaîne de A^* est donc reconnue par l'automate \mathcal{A} si, et seulement si, c'est l'étiquette d'un calcul réussi de \mathcal{A} .

Ici, $q_0 \xrightarrow{abbbbcbdd} q_2$ donc la chaîne $abbbbcbdd$ est reconnue par \mathcal{A} .

À retenir

Si l'automate se bloque pendant la lecture de la chaîne ou n'atteint pas l'état final, cette chaîne n'est pas reconnue par l'automate.

Langage reconnaissable par un automate

On note $\mathcal{L}(\mathcal{A})$ l'ensemble des chaînes reconnues par l'automate :

$$\mathcal{L}(\mathcal{A}) = \left\{ \mu \in A^* \mid \exists q_i \in I, \exists q_t \in T, q_i \xrightarrow{\mu} q_t \right\}$$

Définition 1 - 22

et on dit qu'un langage L est **reconnaisable par l'automate** \mathcal{A} ou que l'automate \mathcal{A} **reconnait** le langage L si, et seulement si, $\mathcal{L}(\mathcal{A}) = L$.

Un langage est **reconnaisable** si, et seulement si, il existe AU MOINS un automate FINI qui le reconnaît.

L'ensemble des langages reconnaissables sur l'alphabet A est noté **Rec**(A^*).

4 3 Langage reconnu par un automate fini

Une première question qui vient à l'esprit en ayant le graphe d'un automate sous les yeux : quel est le langage reconnu par cet automate ?

4 3 1 Méthode « manuelle »

On essaie de déterminer pas à pas la succession de langages permettant de passer des états initiaux aux états terminaux.

En utilisant toujours notre exemple, on voit qu'avec a on passe à l'état q_1 . On peut y rester en bouclant avec des b ou passer à l'état terminal q_2 avec c en bouclant éventuellement avec des d .

Le langage reconnu peut donc s'écrire à l'aide de l'expression rationnelle ab^*cd^* .

4 3 2 Technique d'élimination d'états

On tente cette fois d'éliminer les états intermédiaires pour obtenir un automate à deux états étiqueté par une expression déterminant le langage reconnu. On généralise ainsi les automates étiquetés par des symboles ou des chaînes.

Cette technique est dérivée de l'algorithme de MAC NAUGHTON et YAMADA.

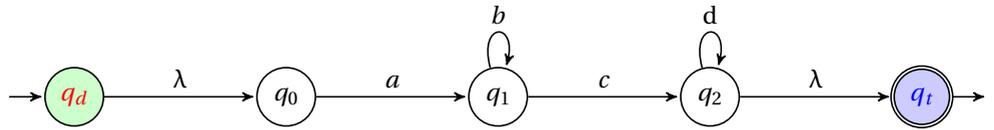
– On commence par créer deux nouveaux états q_d et q_t qui seront les uniques états initiaux et terminaux.

On relie q_d à tous les états initiaux par une transition étiquetée par λ et on relie tous les états terminaux à q_t par le même type de transitions.

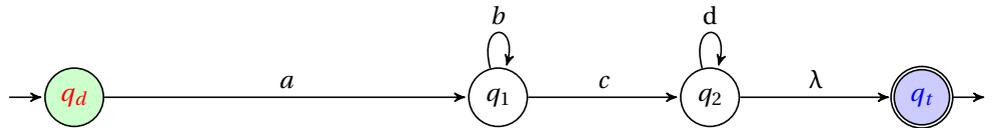
– Notons Q l'ensemble tel que l'alphabet d'états soit $\{q_d\} \cup Q \cup \{q_t\}$. Tant que Q n'est pas vide, on applique l'opération suivante : pour tout couple (p, r) d'états tels qu'il existe une transition directe de p à q et de q à r étiquetée respectivement par L_{pq} et L_{qr} , on crée une transition (p, L_{pqr}, r) avec $L_{pqr} = L_{pr} \cup L_{pq}L_{qr}^*$.

Reprenons notre automate de départ.

– on ajoute q_d et q_f :



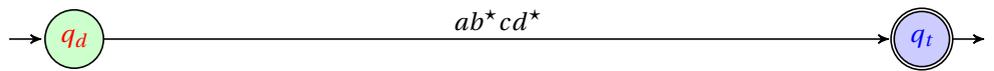
- on élimine l'état q_0 : $L_{d01} = L_{d1} \cup L_{d0}L_{00}^*L_{01} = \emptyset \cup \lambda\lambda^*a = a$



- on élimine l'état q_1 : $L_{d02} = L_{d2} \cup L_{d1}L_{11}^*L_{12} = \emptyset \cup ab^*c = ab^*c$



- on élimine l'état q_2 : $L_{dt} = L_{dt} \cup L_{d2}L_{22}^*L_{2t} = \emptyset \cup ab^*cd^*\lambda = ab^*cd^*$



4 4 Automates équivalents

Automates équivalents

On définit une relation \equiv sur l'ensemble des automates finis.

Deux automates \mathcal{A} et \mathcal{A}' sont en relation si, et seulement si, ils reconnaissent le même langage.

Cette relation est une relation d'équivalence. On note $\mathcal{A} \equiv \mathcal{A}'$ pour signifier que deux automates sont équivalents.

Théorème 1 - 3

Il est assez évident de démontrer que la relation \equiv est une relation d'équivalence. Cette notion est très importante en mathématiques et très utilisée en informatique. Au lieu de considérer les automates finis dans leur ensemble, nous allons nous contenter de parler des **classes d'équivalence** qui sont les éléments de l'ensemble des automates quotienté par \equiv .

Aparté

Pensez justement aux fractions rationnelles qui renvoient naturellement à la notion de quotient : $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}$, etc. sont des « représentants » de la classe d'équivalence de $(1, 2)$ pour la relation définie par $(a, b)\mathcal{R}(x, y) \Leftrightarrow ay = bx$ sur $\mathbb{Z} \times \mathbb{Z}$. L'ensemble quotient $\mathbb{Z} \times \mathbb{Z} / \mathcal{R}$ est justement l'ensemble... \mathbb{Q} !

La classe de $(1, 2)$ est $\{\dots, \frac{-2}{4}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots\}$.

Deux automates pourront donc « avoir l'air » différents mais représenteront le même langage. Comme on préfère travailler avec $\frac{1}{2}$ plutôt qu'avec $\frac{2134}{4268}$, on essaiera de simplifier au maximum un automate pour débusquer plus facilement le langage qu'il reconnaît.

4 5 Automates standards

Définition 1 - 23

Automate standard

Un automate $\langle A, Q, D, T, \tau \rangle$ est standard si, et seulement si, D est réduit à un singleton $\{d\}$ et aucune transition n'aboutit en d .

L'algorithme suivant va nous permettre de rendre standard tout automate fini. Notons \mathcal{A}' l'automate standardisé, alors $\mathcal{A}' = \langle A, Q \cup \{d\}, \{d\}, T', \tau' \rangle$ avec :

- $d \notin Q$;
- si $D \cap T = \emptyset$ alors $T' = T$ sinon $T' = T \cup \{d\}$;
- $\mathcal{G}_{\tau'} = \mathcal{G}_{\tau} \cup \{(d, a, q) \mid \exists q_d \in D, (q_d, a, q) \in \mathcal{G}_{\tau}\}$

Cela nous permet d'énoncer le théorème suivant :

Théorème 1 - 4

Tout automate fini est équivalent à un automate standard.

Ou bien « toute classe d'équivalence pour \equiv contient un automate standard ».

Recherche

Standardisez l'automate défini sur l'alphabet $\{a, b\}$ par la table de transition suivante :

τ	a	b
q_0	q_1	
q_1	q_1	q_0, q_2
q_2	q_0	q_2

avec $D = Q$ et $T = \{q_0\}$.

4 6 Automates émondés

Ouvrons le dictionnaire :

ÉMONDER v. tr. (lat. *emundare*, de *mundus*, propre; v. 1200, « purifier »). **1.** (1354). Couper les branches inutiles : *Émonder un peuplier*. — **2.** Débarrasser du superflu : *Émonder un récit des détails inutiles*.

Tout est dit...Enfin, pour avoir quelque chose de plus rigoureux afin de l'utiliser informatiquement, donnons quelques définitions intermédiaires.

Définition 1 - 24

États accessibles et co-accessibles

Soit $\mathcal{A} = \langle A, Q, D, T, \tau \rangle$ un automate fini.

- On dit que l'état q_j ($q_j \in Q$) est **accessible à partir d'un état** q_i ($q_i \in Q$) s'il existe (au moins) un calcul c dans \mathcal{A} dont l'origine est q_i et l'extrémité est q_j . On dit que l'état q_j est **accessible** s'il est accessible à partir d'un état initial.
- Un état q_i est **co-accessible à un état** q_j s'il existe un calcul c dans \mathcal{A} dont l'origine est q_i et l'extrémité est q_j . On dit que l'état e_i est **co-accessible** s'il est co-accessible d'un état final.
- On dit qu'un état q_i est **utile** s'il est à la fois accessible et co-accessible.

Ceci nous permet de définir un automate émondé :

Définition 1 - 25

Automate émondé

Un automate émondé est un automate dont tous les états sont utiles.

On peut définir deux algorithmes servant à émonder un automate donné. Il s'agit de supprimer les états non accessibles ou non co-accessibles et les transitions qui en dépendent. On considère toujours notre automate fini $\mathcal{A} = \langle A, Q, D, T, \tau \rangle$.

Fonction émondage aller($\mathcal{A} : \text{automate fini}$) : *automate fini*

Début

$E \leftarrow D$

$E' \leftarrow \emptyset$

TantQue $E' \neq E$ **Faire**

$E' \leftarrow E$

$E \leftarrow E \cup \{q \in Q \mid \exists e \in E, \exists a \in A : (e, a, q) \in \mathcal{G}_\tau\}$

FinTantQue

Retourner $\langle A, E, D, T, \tau' \rangle$

Fin

Fonction émondage retour($\mathcal{A} : \text{automate fini}$) : *automate fini*

Début

$C \leftarrow T \cap E$

$C' \leftarrow \emptyset$

TantQue $C' \neq C$ **Faire**

$C' \leftarrow C$

$C \leftarrow C \cup \{q \in Q \mid \exists c \in C, \exists a \in A : (q, a, c) \in \mathcal{G}_\tau\}$

FinTantQue

Retourner $\langle A, C, D, T, \tau'' \rangle$

Fin

Standardisez et émondez l'automate défini sur l'alphabet $\{a, b\}$ à l'aide de la table de transition suivante :

τ	a	b
q_1	q_1, q_2	
q_2		q_3
q_3	q_3	q_3
q_4	q_3	q_2

avec $D = \{q_1, q_3\}$ et $T = \{q_1, q_2\}$

Recherche

On peut montrer qu'éliminer les états qui ne sont pas utiles ne change pas le langage reconnu par un automate et donc :

Théorème 1 - 5

Tout automate fini est équivalent à un automate émondé

ou bien « toute classe d'équivalence pour \equiv contient un automate émondé ».

4 7 Automates déterministes

Définition 1 - 26

Un automate *déterministe* :

- a un unique état initial ;
- la relation de transition τ est une fonction : il y a, à partir de chaque état, au plus une transition d'étiquette donnée.

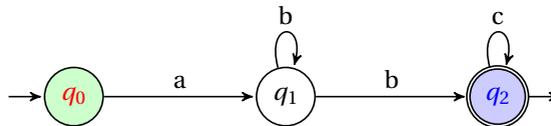
Si un automate n'est pas déterministe, il est...non-déterministe.

Définition 1 - 27

Un automate *déterministe complet* :

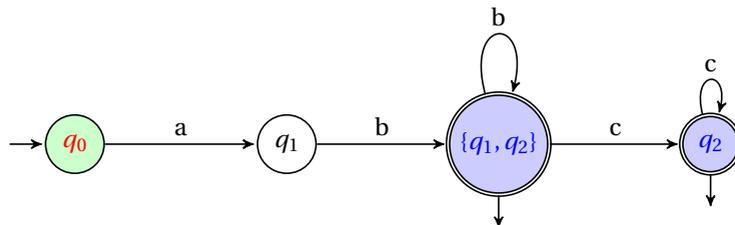
- est un automate déterministe ;
- la relation de transition τ est une application : il y a, à partir de chaque état, une et une seule transition d'étiquette donnée.

Par exemple :



n'est pas déterministe car (q_1, b) admet deux images par τ qui sont q_1 et q_2 .

Il est possible de rendre cet automate déterministe en regroupant toutes les images d'un couple donné en un seul état :



Théorème 1 - 6

Tout automate fini est équivalent à un automate déterministe.

ou bien, « toute classe d'équivalence pour \equiv » contient un automate déterministe.

Le problème d'un automate non déterministe est qu'il est moins efficace. Dans le cas d'un automate déterministe, pour chaque chaîne reconnue, il existe un unique calcul dont cette chaîne est l'étiquette.

Voici un algorithme qui permet de manière assez économique d'obtenir un automate déterministe équivalent à un automate donné.

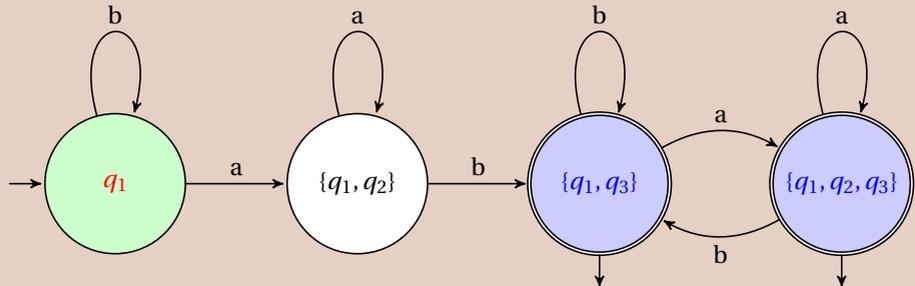
Considérons un automate non déterministe $\mathcal{A} = \langle A, Q, \{d\}, T, \tau \rangle$ mais standard et notons $\mathcal{A}^D = \langle A, Q^D, \{d\}, T^D, \tau^D \rangle$ l'automate construit de la manière suivante :

- au départ, $Q^D \leftarrow \{d\}$;
- on détermine les images non vides de chaque couple $(\{d\}, a)$ pour chaque a dans A . On obtient de nouveaux états q_i^D que l'on met dans Q^D ;
- on recommence ainsi avec les images des (q_i^D, a) pour chaque a dans A ;
- on s'arrête quand on ne crée plus de nouveaux états ;
- T^D est l'ensemble des q_i^D qui contiennent un état terminal de \mathcal{A} .

Vérifiez que l'algorithme précédent permet de montrer que l'automate défini par :

τ	a	b
q_1	q_1, q_2	q_1
q_2		q_3
q_3	q_3	q_3

avec $I = \{q_1\}$ et $T = \{q_3\}$ est équivalent à :



Recherche

4 8 Opérations rationnelles sur les automates

4 8 1 Union

Soit $\mathcal{A}_1 = \langle A, Q_1, D_1, T_1, \tau_1 \rangle$ et $\mathcal{A}_2 = \langle A, Q_2, D_2, T_2, \tau_2 \rangle$ deux automates finis reconnaissant deux langages L_1 et L_2 . On peut supposer que $Q_1 \cap Q_2 = \emptyset$ quitte à renuméroter les états (en effet les noms des états n'ont aucune importance). Alors on définit un nouvel automate

$$\mathcal{A}_1 + \mathcal{A}_2 = \langle A, Q_1 \cup Q_2, D_1 \cup D_2, T_1 \cup T_2, \tau_1 \cup \tau_2 \rangle$$

en notant abusivement $\tau_1 \cup \tau_2$ la relation de graphe $\mathcal{G}_{\tau_1} \cup \mathcal{G}_{\tau_2}$.

Théorème 1 - 7

L'automate $\mathcal{A}_1 + \mathcal{A}_2$ reconnaît le langage $L_1 + L_2$.

En général, il est ensuite nécessaire de rendre cet automate standard et émondé.

4 8 2 Produit

Soit $\mathcal{A}_1 = \langle A, Q_1, D_1, T_1, \tau_1 \rangle$ et $\mathcal{A}_2 = \langle A, Q_2, D_2, T_2, \tau_2 \rangle$ deux automates finis reconnaissant deux langages L_1 et L_2 . On peut supposer que $Q_1 \cap Q_2 = \emptyset$. Quitte à standardiser \mathcal{A}_2 , on peut supposer que $D_2 = \{d_2\}$.

On définit alors un nouvel automate :

$$\mathcal{A}_1 \cdot \mathcal{A}_2 = \langle A, (Q_1 \cup Q_2) \setminus \{d_2\}, D_1, T', \tau_1 \cup \tau_2' \cup \tau_2'' \rangle$$

avec :

- $T' = (T_1 \cup T_2) \setminus \{d_2\}$ si $d_2 \in T_2$ et $T_1 \cup T_2$ sinon ;
- $\mathcal{G}_{\tau'_2} = \{(q, a, q') \in \text{GR}_{\tau_2} \mid q \neq d_2\}$;
- $\mathcal{G}_{\tau'_2} = \{(q_{t_1}, a, q') \mid q_{t_1} \in T_1, (d_2, a, q') \in \mathcal{G}_{\tau_2}\}$.

Recherche

Comment décrire concrètement la construction de $\mathcal{A}_1 \cdot \mathcal{A}_2$?

Théorème 1 - 8

L'automate $\mathcal{A}_1 \cdot \mathcal{A}_2$ reconnaît le langage $L_1 \cdot L_2$.

4 8 3 Étoile

Soit $\mathcal{A} = \langle A, Q, \{d\}, T, \tau \rangle$ un automate fini *standard* reconnaissant un langage L .
On définit alors un nouvel automate

$$\mathcal{A}^* = \langle A, Q, \{d\}, T \cup \{d\}, \tau' \rangle$$

avec $\text{GR}_{\tau'} = \mathcal{G}_\tau \cup \{(q_t, a, q) \mid q_t \in T, (d, a, q) \in \mathcal{G}_\tau\}$

Recherche

Comment décrire concrètement la construction de \mathcal{A}^* ?

Théorème 1 - 9

L'automate \mathcal{A}^* reconnaît le langage L^* .

4 9 Théorème de Kleene

Nous pouvons déduire de ce qui précède que tout langage rationnel est reconnaissable par un automate.

En fait, la réciproque est vraie aussi mais assez compliquée à démontrer. Ces deux résultats constituent le théorème de KLEENE :

Théorème 1 - 10

Théorème de KLEENE (1956)

Pour tout alphabet A , $\text{Rat}(A^*) = \text{Rec}(A^*)$.

Ainsi, si un langage peut être décrit par une expression rationnelle, alors il existe un automate fini qui le reconnaît.

Réciproquement, si un langage est reconnaissable, alors il existe une expression rationnelle qui le décrit.

Notez bien que certains langages ne sont pas reconnaissables, comme par exemple l'ensemble des chaînes sur $\{A, B\}$ constituées d'autant de a que de b . En raisonnant par l'absurde, n peut montrer qu'aucun automate *fini* ne peut reconnaître ce langage.

4 10 Automate associé à un langage défini par une expression rationnelle

4 10 1 Méthode « manuelle »

Une expression rationnelle correspond à une construction récursive à partir d'opérations simples sur des langages réduits à des singletons et les constructions précédentes vont nous permettre de construire petit à petit un automate fini correspondant.

4 10 2 Algorithme de Glushkov

La méthode suivante est attribuée à l'informaticien soviétique Viktor GLUSHKOV qui l'a proposée en 1961. Il construit un automate ayant un état de plus que le nombre de symboles qui apparaissent dans l'expression rationnelle.

On *linéarise* l'expression rationnelle, i.e., on remplace tous les caractères par des symboles distincts, numérotés à partir de 1 de la gauche vers la droite.

Par exemple, $ab^* + a^2b^+$ devient $x_1x_2^* + x_3x_4x_5^+$.

On crée ensuite un état par variable ainsi qu'un état q_0 qui représente l'état initial.

On crée l'ensemble posliedny (dernier en russe) qui contient tous les caractères pouvant terminer une chaîne plus éventuellement l'état q_0 si λ appartient au langage : il constitue l'ensemble des états terminaux de l'automate.

On crée l'ensemble piervy (premier en russe) des caractères pouvant commencer un mot : on relie l'état q_0 à chaque q_i de cet ensemble en l'étiquetant par x_i .

On crée une transition étiquetée par x_j de l'état q_i vers l'état q_j si le facteur x_ix_j peut apparaître dans au moins une chaîne du langage.

Finalement, on remplace les x_i par les caractères qu'ils remplaçaient.

Il ne reste plus qu'à s'occuper d'une vingtaine d'exemples...

4 11 Automates à états finis avec sortie

Pour modéliser de nouvelles situations, il faut sortir du cadre restreint des automates à états finis sans sortie. Voici une première catégorie qui diffère peu de la précédente, à un petit détail près...

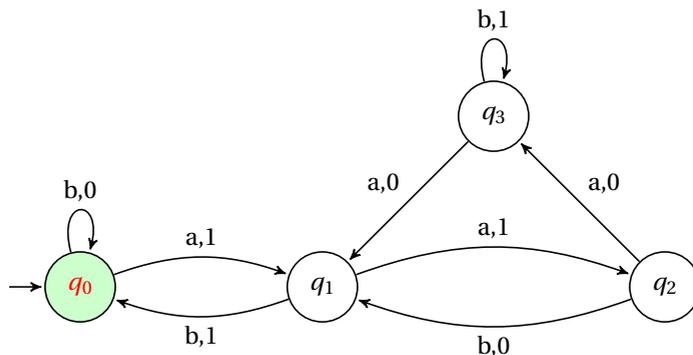
Un automate à états finis avec sorties est caractérisé par un sextuplet $\langle Q, q_0, A_I, A_S, f_t, f_s \rangle$ où :

- Q est un ensemble fini d'états ;
- q_0 est l'état initial ;
- A_I est l'alphabet d'entrée ;
- A_S est l'alphabet de sortie ;
- f_t est la fonction de transition de $Q \times A_I$ vers Q ;
- f_s est la fonction de sortie de $Q \times A_I$ vers A_S .

Définition 1 - 28

Vous aurez bien noté que l'automate ne contient qu'un seul état initial et que les fonctions de transition et de sortie sont des...fonctions, if you see what I mean...

Pour représenter l'automate par un diagramme, on étiquette chaque transition par un caractère d'entrée suivi du caractère de sortie correspondant.



Par exemple, la chaîne d'entrée babaaaaabbba donne en sortie 0111100101110.

4 12 Automates à pile

On a déjà évoqué le cas du langage $\{0^n 1^n \mid n \in \mathbb{N}\}$ qui ne peut être reconnu par aucun automate fini. Il existe des automates plus généraux qui reconnaissent ce genre de langages.

Pour définir un automate à pile nous avons besoin :

1. d'un alphabet $A = \{\dots, \alpha_z, \dots\}$, rappelons que A est forcément fini et non vide ; c'est sur cet alphabet que nous allons construire des mots ;
2. de savoir ce qu'est une pile, bien que cette pile soit rechargeable, elle ne peut en aucun cas être utilisée pour remplacer la pile de votre calculatrice le jour d'un examen. Pour simplifier une pile est une liste ordonnée d'éléments - cette liste peut être vide - sur laquelle deux opérations élémentaires peuvent être réalisées :
 - insertion d'un élément au sommet de la pile (empiler)
 - suppression de l'élément au sommet de la pile (dépiler)
 il est alors clair que le premier élément empilé sera le dernier à être dépilé ; C'est pourquoi « pile » est un synonyme de FILO (First In Last Out) ou de LIFO (Last In First Out).
3. d'un alphabet de pile $P = \{p_1, p_2, p_3, \dots\}$, c'est tout simplement un ensemble fini de symboles spécifiques à la pile ; la pile va nous servir à mémoriser des étapes et, pour savoir où on en est ou ce qui a été fait avant, on va regarder l'état de la pile pour continuer ;
4. d'un ensemble d'états $E = \{e_1, e_2, \dots\}$, $s \in E$ est l'unique état initial de l'automate ; on note T la partie de E constituée des états terminaux, on dit aussi acceptants ;
5. μ est la relation de transition, c'est une relation :

$$(E \times (P \cup \{\lambda\})) \times (A \cup \{\lambda\}) \longrightarrow E \times (P \cup \{\lambda\})$$

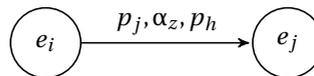
une transition est alors assimilée à un triplet (comme pour les automates à états finis). Si (e_k, p_h) est une image de $((e_i, p_j), \alpha_z)$ par μ on note

$$((e_i, p_j), \alpha_z, (e_k, p_h))$$

qui se lit : « si l'automate est dans l'état e_i et que le sommet de la pile est p_j et que l'automate lit α_z alors l'automate passe dans l'état e_k , dépile p_j de la pile et empile p_h ». Si $p_j = \lambda$ on ne s'occupe pas de savoir ce qu'il y a au sommet de la pile et on ne dépile rien, si $p_h = \lambda$ cela indique que l'on n'empile rien. La possibilité de pouvoir avoir $\alpha_z = \lambda$ nous permet, en cas de besoin, de modifier l'état de l'automate et du sommet de pile.

On le remarque immédiatement, un état d'un automate à pile n'est jamais isolé dans une transition, il doit être associé à un symbole de pile (ou λ), les états de notre automate sont alors des couples.

Comme pour les automates à états finis, α_z est l'étiquette de la transition :



On généralise cette définition en autorisant dans les transitions l'empilement d'une chaîne de plusieurs symboles de la pile :

$$((e_i, p_j), \alpha_z, (e_k, M))$$

ici on va empiler tous les symboles de M qui est un mot sur P l'alphabet de pile.

On peut, au lieu de présenter les transitions sous la forme $((e_i, p_j), \alpha_z, (e_k, p_h))$, utiliser lorsque μ est une fonction

$$\mu(e_i, p_j, \alpha_z) \text{ ou } \mu((e_i, p_j), \alpha_z) = (e_k, p_h)$$

qui se lit évidemment encore : si l'automate est dans l'état e_i et qu'il y a p_j en sommet de pile (si $p_j = \lambda$ on ne s'occupe pas du sommet de pile et on ne dépilera rien) et que l'automate lit α_z alors il passe dans l'état e_k , on dépile p_j et on empile p_h .

On dit qu'un mot m de A^* est reconnu par l'automate s'il existe une suite de transitions partant de l'état initial et pile vide dont la suite des étiquettes est m et aboutissant à un état final ou acceptant et pile vide. L'ensemble des mots reconnus par l'automate à pile est le langage engendré ou reconnu par cet automate.

Considérons l'automate défini par

$$A = \{a, b\}, E = \{s, 1, 2\}, T = \{2\}, P = \{u\}$$

et les transitions

$$T_1 : ((s, \lambda), a, (1, u))$$

$$T_2 : ((1, \lambda), a, (1, u))$$

$$T_3 : ((1, u), b, (2, \lambda))$$

$$T_4 : ((2, u), b, (2, \lambda))$$

T_1 : pour démarrer, l'automate doit être dans l'état initial s (c'est le seul état initial) et la pile doit être vide, si c'est le cas et qu'il lit a alors il passe dans l'état 1, on ne dépile rien (λ) et on empile u .

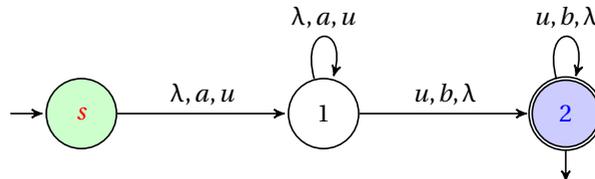
T_2 : si l'automate est dans l'état 1 et qu'il lit a alors il reste dans l'état 1, on ne dépile rien (λ) et on empile u .

T_3 : si l'automate est dans l'état 1 et que le sommet de la pile est u et qu'il lit b alors il passe dans l'état 2, on dépile u (le sommet de la pile) et on n'empile rien (λ).

T_4 : si l'automate est dans l'état 2 et que le sommet de la pile est u et qu'il lit b alors il passe (il reste) dans l'état 2, on dépile u (le sommet de la pile) et on n'empile rien (λ).

Vous aurez remarqué que la relation μ est une fonction, on dit dans ce cas que l'automate à pile est déterministe.

L'état de sortie de l'automate est ici l'état 2 ($T = \{2\}$) mais on ne peut utiliser cette sortie qu'au moment où la pile est vide.



On remarque assez facilement qu'à chaque fois que l'automate lit un a , on empile un u , il y aura alors dans la pile autant de u que de a lus ; à chaque fois que l'automate lit un b on dépile un u (si ce n'est pas possible, l'automate ne peut lire b), en conséquence l'automate sera dans l'état 2 avec la pile vide lorsqu'il aura lu autant de b que de a . Le langage reconnu par cet automate est $\{a^n b^n \mid n \in \mathbb{N}^*\}$, la pile nous permet de mémoriser le nombre de a lus ce que ne permet pas un automate à états finis.

Si nous décidons que s est aussi un état final et comme au départ la pile est vide, on conclut, comme pour les automates à états finis, que λ fait partie du langage reconnu par l'automate.

Si on veut que la pile soit vide à un certain état e_i , pour vider la pile il suffit de rajouter les transition $((e_i, p), \lambda, (e_i, \lambda))$ avec p un symbole de pile quelconque.

4 13 Machines de Turing : le retour

On peut montrer qu'un automate à pile ne peut reconnaître le langage $\{0^n 1^n 2^n \mid n \in \mathbb{N}\}$: il faut imaginer quelque chose de plus puissant comme...les machines de TURING. La boucle est bouclée, les machines de TURING sont l'alpha et l'oméga de l'informatique théorique...

5

Présentation générale de la logique des propositions

On appellera **proposition** tout énoncé dont on peut décider s'il est vrai ou faux indépendamment de ses composantes.

On distinguera la logique des propositions de la logique des **prédicats** qui introduit des variables dans les assertions qui peut les rendre donc parfois vraies et parfois fausses et que nous étudierons en deuxième année.

Par exemple « *Igor dort* » est une proposition susceptible d'être vraie ou fausse dans toute situation alors que la valeur de vérité de « *x dort* » dépend de x .

Nous distinguerons également la **syntaxe** de la logique des propositions de sa SÉMANTIQUE. Le dictionnaire propose les définitions suivantes :

- **syntaxe** : n. f. (bas latin syntaxis, du grec suntaxis, ordre) Partie de la grammaire qui décrit les règles par lesquelles les unités linguistiques se combinent en phrases.
- **sémantique** : n. f. (bas latin semanticus, du grec sēmantikos, qui signifie) **1.** Étude du sens des unités linguistiques et de leurs combinaisons. **2.** Étude des propositions d'une théorie déductive du point de vue de leur vérité ou de leur fausseté.

L'étude de l'aspect syntaxique consiste à préciser comment l'on construit les formules et l'aspect sémantique interprète les formules en terme de *Vrai* ou *Faux*.

5 1 Syntaxe

5 1 1 Les symboles

L'alphabet du langage de la logique des propositions est constitué de :

- un ensemble fini ou infini dénombrable de *variables propositionnelles*;
- la constante logique \perp qui se lit « FAUX »;
- les *connecteurs* \neg (non), \wedge (et), \vee (ou), \rightarrow (implique) et \leftrightarrow (équivalent) ;
- les parenthèses « (» et «) ».

Le connecteur \neg est un *connecteur unaire* et les autres sont des *connecteurs binaires*.

L'ensemble des formules de la logique propositionnelle est le plus petit ensemble \mathcal{F} tel que :

- toute variable propositionnelle est un élément de \mathcal{F} ;
- \perp est un élément de \mathcal{F} ;
- si $p \in \mathcal{F}$, alors $(\neg p) \in \mathcal{F}$;
- si p et q sont dans \mathcal{F} , alors $(p \wedge q)$, $(p \vee q)$, $(p \rightarrow q)$, et $(p \leftrightarrow q)$ sont des éléments de \mathcal{F} .

Par exemple, $s \rightarrow ((p \vee (\neg q)) \vee (p \vee (\neg r)))$ est une proposition mais $\neg \wedge (p) \vee$ ne l'est pas.

On peut se passer de quelques parenthèses en adoptant les règles de priorité suivantes :

- \neg est prioritaire sur les autres opérateurs ;
- \vee et \wedge sont prioritaires sur \rightarrow et \leftrightarrow .

Mais attention ! $p \vee q \wedge r$ est ambigu.

5 1 2 Démonstration par induction

Si une propriété P portant sur les formules de \mathcal{F} est telle que :

- toute variable propositionnelle vérifie P ;
 - \perp vérifie P ;
 - si la formule p vérifie P , alors $(\neg p)$ vérifie P ;
 - si p et q vérifient P , alors $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$ et $(p \leftrightarrow q)$ vérifient P ;
- alors toutes les formules de \mathcal{F} vérifient P .

Théorème 1 - 11

Ce théorème permet par exemple de prouver le théorème suivant :

Théorème 1 - 12

Toute formule de \mathcal{F} a autant de parenthèses ouvrantes que de parenthèses fermantes.

La preuve est laissée en exercice.

5 1 3 Sous-formules

Nous n'entrerons pas dans les détails mais on peut définir par induction les sous-formules d'une formule donnée : on retiendra juste qu'il s'agit de toutes les formules apparaissant dans une formule donnée.

Par exemple, l'ensemble des sous-formules de $(p \rightarrow q) \vee \neg(q \leftrightarrow r)$ est

$$\{p \rightarrow q, \neg(q \leftrightarrow r), q \leftrightarrow r, p, q, r\}$$

5 2 Sémantique

5 2 1 Valeurs et tables de vérité

On considère un ensemble $\mathcal{B} = \{0, 1\}$ ou $\{F, V\}$ ou $\{\text{Oui}, \text{Non}\}$, etc.

Une *distribution des valeurs de vérité* est une application v de \mathcal{F} dans \mathcal{B} définie inductivement par :

- $v(\perp) = 0$,
 - $v(\neg p) = 1$ si, et seulement si, $v(p) = 0$;
 - $v(p \wedge q) = 1$ si, et seulement si, $v(p) = v(q) = 1$;
 - $v(p \vee q) = 0$ si, et seulement si, $v(p) = v(q) = 0$;
 - $v(p \rightarrow q) = 0$ si, et seulement si, $v(p) = 1$ et $v(q) = 0$;
 - $v(p \leftrightarrow) = 1$ si, et seulement si, $v(p) = v(q)$,
- avec p et q des éléments quelconques de \mathcal{F} .

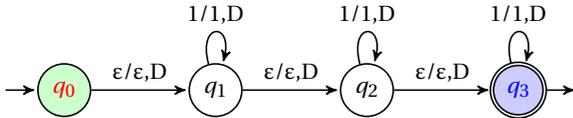
Définition 1 - 29

EXERCICES

Machines de Turing

Exercice 1 - 1

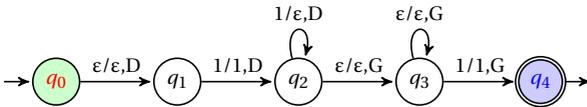
On considère la machine de TURING représentée par l'automate ci-dessous qui est dans l'état initial $q_0 \in 1111 \varepsilon 111111 \varepsilon 111111 \varepsilon 111 \varepsilon 1111 \varepsilon 111011 \varepsilon$:



Quelle est la configuration finale de la machine ?

Exercice 1 - 2

Quelle est la configuration finale de la machine de TURING décrite par l'automate suivant sachant que la configuration initiale du ruban est $q_0 \varepsilon \bar{x} \varepsilon$ (on rappelle que la représentation unaire d'un nombre x est noté \bar{x}) :



Exercice 1 - 3

Construire une machine de TURING qui calcule la fonction prédécesseur.

Exercice 1 - 4

Comment s'écrit 0 en système unaire ? Construire une machine de TURING qui calcule la fonction identiquement nulle : la configuration initiale est $q_0 \varepsilon \bar{x} \varepsilon$ et la configuration finale est $q_f \varepsilon 1 \varepsilon$

Exercice 1 - 5

Nous allons construire une machine à additionner. En base 1, c'est assez simple : écrivez l'addition en base 1 de 4 et 1 puis de 4 et 0.

On suppose qu'on a marqué en entrée $\varepsilon \bar{x} \varepsilon \bar{y} \varepsilon$ avec x et y les deux nombres à additionner.

La configuration finale attendue est $q_f \varepsilon \overline{x+y} \varepsilon$.

Exercice 1 - 6

Voici les codes ASCII décimaux de quelques caractères affichables :

Caractère	A	B	C	D	E	F	G	H	I	J
Code	65	66	67	68	69	70	71	72	73	74

Caractère	a	b	c	d	e	f	g	h	i	j
Code	97	98	99	100	101	102	103	104	105	106

1. Écrire les valeurs en base 2 des codes de A, B et C puis a, b et c.
2. Déterminer un automate décrivant une machine de TURING la plus simple possible qui transforme le code ASCII (en binaire) d'une lettre minuscule en le code ASCII (en binaire toujours) de la majuscule correspondante.

Fonctions récursives

Exercice 1 - 7

Soit g la fonction projection $\pi_1^{(1)}$ et $h = s \circ \pi_3^{(3)}$ avec s la fonction successeur.

Soit f la récurrence de base g et de pas h définie sur \mathbb{N}^2 .

Calculer $f(0,0)$, $f(0,1)$, $f(1,1)$, $f(2,1)$, $f(1,2)$, $f(4,2)$, $f(2,4)$.

A-t-on $f(x,y) = f(y,x)$ pour tout couple (x,y) d'entiers ?

Exercice 1 - 8

Voici quelques fonctions écrites sous Python :

```
def succ(x):
    return x+1

def pred(x):
    if x == 0:
        return 0
    else:
        return x-1

def pi(k,T):
    return T[k-1]

def g(x):
    return x

def h(T):
    return succ(pi(3,T))

def A(x1,x2):
    if x2 == 0:
```

```

return g(x1)
else:
return h([x1, x2, A(x1, pred(x2))])

```

Que va retourner $A(2, 3)$?

De quels types sont les arguments \mathbf{x} , \mathbf{T} , $\mathbf{x1}$ dans les différentes fonctions ci-dessus ?

Exercice 1 - 9

Soit g la fonction identiquement nulle et h définie par $h(x, y, z) = \text{add}(\pi_1^{(3)}(x, y, z), \pi_3^{(3)}(x, y, z))$ avec add la fonction d'addition définie en cours.

Soit f la fonction définie sur \mathbb{N}^2 par :

$$\begin{cases} f(x, 0) = 0 \\ f(x, y + 1) = \text{add}(x, f(x, y)) \end{cases}$$

Montrer que f peut être définie comme la récurrence de base g et de pas h avec g et h des fonctions primitives récursives définies à partir des fonctions de base. Calculer $f(0, 0)$, $f(0, 1)$, $f(1, 1)$, $f(2, 1)$, $f(1, 2)$, $f(4, 2)$, $f(2, 4)$.

Que pensez-vous de f ?

Exercice 1 - 10

On définit sur Python une nouvelle fonction à partir de la définition vue à l'exercice précédent et de la fonction A définie à l'exercice [Exercice 1 - 8 page précédente](#) :

```

def M(x1, x2):
    if x2 == 0:
        return 0
    else:
        return A(x1, M(x1, pred(x2)))

```

Que pensez-vous de la fonction suivante :

```

def E(x1, x2):
    if x2 == 0:
        return 1
    else:
        return M(x1, E(x1, pred(x2)))

```

On peut continuer ainsi :

```

def T(x1, x2):
    if x2 == 0:
        return 1
    else:
        return E(x1, T(x1, pred(x2)))

```

Comment écririez-vous $\mathbf{T}(2, 4)$? Quel nombre va renvoyer Python ?

Remarque : *quand on passe sur machine, on atteint vite les limites de Python quant au nombre de récursions, même en augmentant cette limite avec `setrecursionlimit(10000)` par exemple.*

Pour travailler confortablement avec des fonctions récursives, on peut employer des langages pour qui ce mode de programmation est « naturel » comme Caml, Scheme, Haskell.



On peut itérer ce genre de construction pour obtenir la famille des puissances itérées de KNUTH, du nom du célèbre auteur de *The Art of computer programming* et du langage $\text{T}_{\text{E}}\text{X}$ entre autres...

Quelques citations :

Computer programming is an art, because it applies accumulated knowledge to the world, because it requires skill and ingenuity, and especially because it produces objects of beauty. A programmer who subconsciously views himself as an artist will enjoy what he does and will do it better.

Ou encore :

The psychological profiling [of a programmer] is mostly the ability to shift levels of abstraction, from low level to high level. To see something in the small and to see something in the large.

On utilise en général les notations suivantes :

$$a \uparrow^n b = \begin{cases} a^b & \text{si } n = 1 \\ 1 & \text{si } b = 0 \\ a \uparrow^{n-1} (a \uparrow^n (b - 1)) & \text{sinon} \end{cases}$$

Exercice 1 - 11

Montrer que la fonction $f : \mathbb{N}^2 \rightarrow \mathbb{N}$ définie par $f(x, y) = xy + 3x^2 + 1$ est primitive récursive.

Exercice 1 - 12

Définissez récursivement la fonction sgn définie sur \mathbb{N} et qui vaut 0 en 0 et 1 sinon.

Définissez récursivement la fonction cosgn définie sur \mathbb{N} et qui vaut 1 en 0 et 0 sinon.

Définissez récursivement la soustraction propre définie sur \mathbb{N} par :

$$\begin{cases} \text{sous}(x, y) = x - y & \text{si } x \geq y \\ \text{sous}(x, y) = 0 & \text{si } x < y \end{cases}$$

à l'aide de la fonction pred .

Montrez alors que les tests $(x < y)$, $(x > y)$ et $x = y$ sont des fonctions primitives récursives en utilisant `sgn`, `cosgn`, `sous` et `add`.

Exercice 1 - 13

1. Calculez quelques termes de la suite d'ACKERMANN.
2. Proposez une fonction Python traduisant littéralement la définition récursive de la fonction d'ACKERMANN. Placez-y un « espion » qui compte le nombre d'appels. Testez sur l'image de (3,6).
3. Commentez le programme suivant :

```
def f(a,b):
    global espion
    espion += 1
    while a > 0:
        if b == 0:
            b = 1
        else:
            b = f(a, b - 1)
        a -= 1
    return b + 1
```

4. Démontrer (éventuellement par récurrence) que :
 - a. $A(0, n) = n + 1$
 - b. $A(1, n) = n + 2$
 - c. $A(2, n) = 2n + 3$
 - d. $A(3, n) = 2^{n+3} - 3$
5. Utilisez tous ces résultats afin d'obtenir une fonction Python plus efficace. Par exemple, calculez $A(4,2)$. Comme Python va calculer avec des grands entiers, vous utiliserez la commande `long` :

```
>>> A(long(4), long(2))
```

Vous vérifierez que $A(4,2)$ est un nombre dont l'écriture décimale comporte 19 729 caractères... Quel est le lien entre la fonction d'ACKERMANN et les puissances itérées de KNUTH ? Comment alors exprimer $A(4, n)$, $A(5, n)$, etc. à l'aide des puissances itérées de KNUTH ?

Langages

Exercice 1 - 14

A est un alphabet :

1. Qu'est-ce qu'une chaîne sur A ?
2. Que désigne A^* ?
3. Qu'est-ce qu'un langage sur A ?
4. A est-il un langage sur A ?
5. A^* est-il un langage sur A ?
6. Toute partie de A est-elle un langage sur A ?
7. Qu'est-ce qu'un langage de A^* ?
8. \emptyset est-il un langage sur A ?
9. $\{\lambda\}$ est-il un langage sur A ?

Exercice 1 - 15

$A = \{a, b, c, d, e\}$ est un alphabet.

Expliciter les langages :

1. $L_1 = \{\mu \in A^* \mid |\mu|_c = 0\}$
2. $L_2 = \{\mu \in A^* \mid \mu = a\xi e \text{ avec } \xi \in L_1\}$
3. $L_3 = \{a, bc\} \cdot \{ad\}$
4. $L_4 = (\{a, bc\} \cdot \{ad\}) + (\{a, b, e\} \cdot \{cd, be\})$
5. $L_5 = I_4^0$
6. $L_6 = I_3^2$
7. $L_7 = \{a^n b^p \mid (n, p) \in \mathbb{N}^* \times \mathbb{N}\}$
8. $\{a\}^+$
9. $\{e, d\}^*$
10. $\{e \cdot d\}^* = \{ed\}^*$

Exercice 1 - 16

Soit un alphabet $A = \{a_1, a_2, \dots, a_n\}$ avec $n \in \mathbb{N}^*$.

On rappelle qu'un ensemble E est un sous-monoïde de A^* si :

- $E \subseteq A$;
- E est *stable* par concaténation, c'est-à-dire que la concaténation de deux éléments de E est encore dans E.

Ce sous-monoïde est dit *libre* s'il contient la chaîne vide λ_A .

Les ensembles suivants sont-ils des sous-monoïdes de A^* ? Si oui, sont-ils libres ? (En d'autres termes, sont-ce des langages ?...)

1. L'ensemble E_1 des chaînes de A de longueur paire.
2. L'ensemble E_2 des chaînes de A de longueur impaire.
3. $E_3 = \{(a_1 a_2)^p, p \in \mathbb{N}\}$.

$$4. E_4 = \{a_1^p a_2^p, p \in \mathbb{N}\}.$$

5. L'ensemble E_5 des mots où le nombre d'occurrences de a_1 est égal au nombre d'occurrences de a_2 .

Exercice 1 - 17

$L = \{a, ab, abab\}$ est un langage sur $A = \{a, b, c\}$

1. Expliciter L^2 .
2. Décrire en français le langage L^* .

Exercice 1 - 18

A est un alphabet, L est un langage sur A et μ est une chaîne de A^* . On appelle *résiduel* de L par rapport à μ le langage

$$\mu^{-1}L = \{\xi \in A^* \mid \mu \cdot \xi \in L\}$$

1. Vérifier que $\mu^{-1}L$ est bien un langage.
2. Démontrer que $\lambda \in \mu^{-1}L \Leftrightarrow \mu \in L$.
3. Déterminer $\lambda^{-1}L$.
4. Démontrer que $\nu^{-1}(\mu^{-1}L) = (\mu\nu)^{-1}L$
5. Si $L = \{ab^k \mid k \in \mathbb{N}^*\}$, déterminer $a^{-1}L$.
6. Si $L = \{b^k a \mid k \in \mathbb{N}^*\}$, déterminer $a^{-1}L$.

Exercice 1 - 19

On travaille avec l'alphabet $A = \{0, 1\}$ et L est le langage sur A formé des écritures normalisées des entiers naturels écrits en base 2, i.e. que 0 s'écrit avec 0 et si $n \neq 0$, son écriture en base 2 commence par un 1; on interdit les écritures du type 000001010111. Exprimer L à l'aide de langages de A^* et d'opérations rationnelles.

Exercice 1 - 20

$A = \{a, b, c, d\}$ et $L = \{a^n c b^p \mid (n, p) \in \mathbb{N}^2\}$. Exprimer L à l'aide de parties de A et d'opérations rationnelles.

Exercice 1 - 21

$A = \{a, b, c, d\}$ et L_1 est l'ensemble des chaînes qui s'écrivent uniquement avec des a ou/et des c. Exprimer L_1 à l'aide de parties de A et d'opérations rationnelles.

Exercice 1 - 22

$A = \{a, b, c, d\}$ et L_2 est l'ensemble des chaînes qui s'écrivent uniquement avec des a ou/et des c et qui contiennent une seule fois la lettre b. Exprimer L_2 à l'aide de parties de A et d'opérations rationnelles.

Exercice 1 - 23

Soient a et b deux symboles d'un alphabet A et $\mu \in A^*$. Montrer par récurrence (sur ?) que si $\mu a = b\mu$ alors $a = b$ et $\mu \in \{a\}^*$.

Langages et expressions rationnels

Exercice 1 - 24

Expliciter les langages associés aux expressions rationnelles suivantes :

1. $a(a+b)^*a$
2. $(aa+bb)^*(ab+ba)(aa+bb)^*$
3. $a^*ba^*ba^*ba^*$
4. $(abc)^*$
5. $(abc^*)^*$

Exercice 1 - 25 Vrai ou faux ?

1. $(a^*)^* = a^*$
2. $aa^* = a^*a$
3. $aa^* + \lambda = a^*$
4. $a(b+c) = ab+ac$
5. $(a+b)^* = (a^*+b^*)^*$
6. $a(ba)^* = (ab)^*a$
7. $(a+b)^* = (a^*b^*)^*$
8. $(a+b)^* = a^*(ba^*)^*$
9. $((a+b)^*+c)^* = (a+b+c)^*$

Exercice 1 - 26

Déterminez des expressions régulières correspondant aux définitions suivantes :

1. les chaînes formées de caractères de l'alphabet non accentués, où les caractères sont dans l'ordre alphabétique croissant et inférieurs à f ;
2. les chaînes de bits sans « 0 » ;
3. les chaînes de bits sans « 01 » ;
4. les chaînes de bits sans « 010 » ;
5. les commentaires dans un langage de programmation formés d'une chaîne encadrée par « [# » et « #] », sans « #] » à l'intérieur si ce n'est à l'intérieur d'une chaîne en étant encadré par « " » et « " » ;
6. les chaînes de bits constituées d'un nombre pair de 1.

Exercice 1 - 27 Expressions rationnelles et grep

Nous allons étudier quelques aspects de l'utilitaire **grep** des systèmes UNIX en rapport avec la notion d'expression rationnelle vue en cours.

Nous utiliserons les opérateurs « * » et « \ | » qui correspondent à l'étoile de KLEENE et à la réunion des chaînes.

Il existe également l'opérateur « + » qui correspond à la concaténation de la chaîne avec son étoile ($a^+ \text{ correspond à } a \cdot a^* = a^+$).

Les parenthèses seront précédées d'une contre-oblique : « \ (» et « \) ».

Nous travaillerons sur un fichier **.txt** contenant une chaîne par ligne. Pour signifier à **grep** que nous recherchons des chaînes correspondant en totalité à l'expression rationnelle donnée, nous l'encadrerons entre les symboles « ^ » et « \$ » qui marquent le début et la fin d'une chaîne.

Par exemple, considérons le fichier expressions.txt suivant :

```
a
b
aab
aaabbbb
abbbbbba
aaaaabaaaababababbaaaaaaaaaabb
ababababababbabaaaaaaaa
bbbbbbbbbbba
abbbbbbbbbbbba
aaaaaaabaaaaaaaaaaaaaaaa
```

Considérons la première expression rationnelle de l'exercice **Exercice 1 - 24**, à savoir $a(a+b)^*a$. Sous **grep** cela donne :

```
$ grep ^a\(a|b\) *a$ ./expression.txt
```

On obtient :

```
abbbbbba
ababababababbabaaaaaaaa
abbbbbbbbbbbba
aaaaaaabaaaaaaaaaaaaaaaa
```

Donnez un exemple de commande permettant de n'obtenir que la dernière chaîne, que la cinquième, que la première, que la troisième.

Que renverra $^a*b*a*? ^a*b*a\+?+$?

Que fait le script Bash suivant :

```
#!/bin/sh
# -> coding: utf-8 ->
read -p "Entrez une expression rationnelle " rat
read -p "Entrez une chaîne " chaine
> ./chaine_test.txt
echo $chaine >> chaine_test.txt
```

```

resultat=$(egrep '^$rat$' ./chaine_test.txt)
if [ ${#resultat} -gt 0 ] ; then
    echo Reconnu ;
else
    echo Non_reconnu ;
fi

```

Généralités sur les automates

Exercice 1 - 28 Diagramme d'un automate

Considérons l'automate suivant :

- l'alphabet est $A = \{0, 1\}$;
- $Q = \{q_0, q_1, q_2, q_3, q_4\}$;
- $I = \{q_0\}$;
- $T = \{q_3\}$;
- la fonction de transition est définie par :

τ	0	1
q_0	q_1	q_3
q_1	q_4	q_2
q_2	q_0	q_2
q_3	q_2	q_4
q_4	q_4	q_4

- Dessinez le diagramme correspondant.
 Donnez des chaînes reconnues par l'automate.
 Donnez des chaînes non reconnues par l'automate.
 Que peut-on dire à propos de l'état q_4 ?

Exercice 1 - 29

Pour chacun des automates suivants I (ou T) indique que l'état est initial (ou terminal), l'alphabet est $A = \{a, b\}$ et les états sont nommés à l'aide d'entiers. Donnez une représentation graphique et des chaînes qui appartiennent au langage engendré ou reconnu par chacun des automates suivants :

1.

τ	a	b
1(I)	1, 2	1
2	3	3
3	4	4
4(T)		

2.

τ	a	b
1(I)	2, 3	2
2(T)	3	
3(I, T)		1, 2

3.

τ	a	b
1(I)	2, 3	1
2(T)	1, 2	
3(I)	1, 3	2

Expression rationnelle associée à un automate

Exercice 1 - 30

On considère l'automate A sur l'alphabet $A = \{a, b\}$ qui a pour ensemble d'états $Q = \{e_1, e_2\}$, e_1 étant simultanément état initial et état final. Les transitions de A sont données par le tableau :

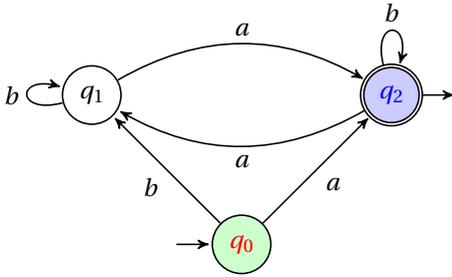
τ	a	b
e_1	e_1	e_2
e_2	e_2	e_1

ce tableau traduit, par exemple, que si l'automate est dans l'état e_2 et qu'il lit b , alors il passe à l'état e_1 .

1. Cet automate est-il déterministe? Justifier votre réponse.
2. Cet automate est-il complet? Justifier votre réponse.
3. Donner une représentation graphique de cet automate.
4. Déterminer une expression rationnelle R qui décrit L.
5. On note L le langage engendré ou reconnu par cet automate, $L = \mathcal{L}(A)$. Ce langage est-il rationnel?
6. λ désigne la chaîne vide. Expliquez pourquoi λ appartient à L.

Exercice 1 - 31

On note L le langage reconnu par cet automate :



Déterminez une expression régulière R qui décrit L.

Automates standards et émondés

Exercice 1 - 32

Standardisez et émondez les automates de l' Exercice 1 - 28 et de l' Exercice 1 - 29.

Exercice 1 - 33

Standardisez l'automate défini sur $A = \{a, b\}$ par :

τ	a	b
q_0	q_1	q_0
q_1	q_0	q_1
q_2	q_2	q_3
q_3	q_3	q_2

sachant que $I = \{q_0, q_2\}$ et $T = \{q_1, q_2\}$.

Exercice 1 - 34

Standardisez et émondez l'automate défini sur $A = \{a, b\}$ par :

τ	a	b
q_0	q_0, q_1	
q_1		q_2
q_2	q_2	q_2
q_3	q_2	q_1

sachant que $I = \{q_0, q_2\}$ et $T = \{q_0, q_1\}$.

Automates déterministes

Exercice 1 - 35

On considère l'automate $A = (A, E, I, T, U)$ avec

- 1. - $A = \{a, b\}$, l'alphabet de l'automate A.

- $Q = \{1, 2, 3\}$ l'ensemble des états de A.
- $I = \{1, 3\}$ l'ensemble des états initiaux de A.
- $T = \{2, 3\}$ l'ensemble des états terminaux de A.
- $U = \{(1, a, 2), (1, a, 3), (1, b, 2), (2, a, 3), (3, b, 1), (3, b, 2)\}$ l'ensemble des transitions de A, U pouvant être représenté par le tableau

τ	a	b
1(I)	2,3	2
2(T)	3	
3(I,T)		1,2

On précise dans ce tableau si un état est initial ou terminal.

- 2. Donnez une représentation graphique de A.
- 3. Déterminez un automate déterministe $A' = (A, E', I', T', U')$ équivalent à A, on présentera U' sous forme d'un tableau.

Exercice 1 - 36

« Déterminez » les automates suivants : I indique que l'état est initial et T que l'état est final

1.

τ	a	b
1(I)	2,3	2
2(T)	3	
3(I,T)		1,2

2.

τ	a	b
1(I)	2	2,3
2(T)		1
3(I,T)	1,2	

3.

τ	a	b
1(I)	2	1,2
2(I)	3	3
3(T)	4	4,1
4(T)		

Construction d'automates

Exercice 1 - 37

Construire des automates correspondant aux expressions rationnelles suivantes :

1. $E = aab^*ab$
2. $E = a^*b^*a^*$
3. $E = a^*bA^+$
4. $E = A^*abcA^*$
5. $E = abA^* + (A^4)^*$
6. $E = (a + aba)^*b(a + b)^*aba(a + b)^*$

Exercice 1 - 38 Identités rationnelles

Tout comme pour les automates, on peut définir une relation d'équivalence sur l'ensemble des expressions rationnelles : deux expressions sont équivalentes si, et seulement si, les langages qui leurs sont associés sont égaux.

L'identité suivante est classique :

$$(a + b)^* \equiv (a^*b)^*a^*$$

Prouvez-la en passant aux automates associés.

Automates à états finis avec sortie

Exercice 1 - 39 avertissement d'erreur de transmission

Un protocole de codage de message prévoit d'indiquer une erreur de transmission si trois 1 apparaissent consécutivement dans le message. Construire un automate à états finis qui renvoie 1 si, et seulement si, la chaîne transmise contient trois 1 consécutifs.

Exercice 1 - 40 automate de rendu de monnaie

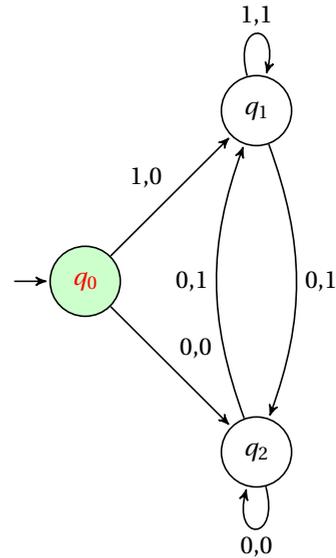
Un distributeur de boisson accepte les pièces de 5, 10 et 20 centimes.

Une fois que l'utilisateur a introduit au minimum 30 centimes, le distributeur lui rend la somme dépassant 30 centimes et il peut choisir entre un café en appuyant sur la touche K ou un lait fraise en appuyant sur la touche L.

Construire un automate à états finis avec sortie qui modélise ce distributeur.

Exercice 1 - 41 Retard

Décrivez le plus précisément possible l'action de cet automate :



Automates à pile

Exercice 1 - 42

Soit l'automate à pile sur l'alphabet $A = \{a, b, \dots\}$ avec :

- $E = \{s, q\}$, s est l'état initial
- $T = \{t\}$
- $P = \{A, B\}$
- les transitions sont :

- | | |
|-------------------------------------|--|
| - $T_1 = ((s, \lambda), a, (s, A))$ | - $T_6 = ((s, B), b, (s, BB))$ |
| - $T_2 = ((s, \lambda), b, (s, B))$ | - $T_7 = ((s, A), a, (t, \lambda))$ |
| - $T_3 = ((s, A), a, (s, AA))$ | - $T_8 = ((s, B), b, (t, \lambda))$ |
| - $T_4 = ((s, B), a, (s, AB))$ | - $T_9 = ((t, A), a, (t, \lambda))$ |
| - $T_5 = ((s, A), b, (s, BA))$ | - $T_{10} = ((t, B), b, (t, \lambda))$ |

1. Donner une représentation graphique de cet automate. On remarquera que cet automate n'est pas déterministe.

2. On note L le langage engendré par cet automate, démontrer que

a. $aaa \in L$

b. $bbbbbb \in L$

c. $aaabaabbaabaaaa \in L$, observer l'état de la pile au fur et à mesure de la reconnaissance du mot.

d. L est un langage particulier sur A en ce sens que tous les mots de L ont une particularité, deviner cette particularité.